



---

# Election Markup Language (EML) Version 5.0

## Process and Data Requirements

### Committee Draft 01

14 March 2007

**Specification URIs:**

**This Version:**

<http://docs.oasis-open.org/election/eml/v5.0/cd01/EML-Process-Data-Requirements-v5.0.doc>  
<http://docs.oasis-open.org/election/eml/v5.0/cd01/EML-Process-Data-Requirements-v5.0.html>  
<http://docs.oasis-open.org/election/eml/v5.0/cd01/EML-Process-Data-Requirements-v5.0.pdf>  
<http://docs.oasis-open.org/election/eml/v5.0/cd01/EML-v5.0-cd01.zip>

**Previous Version:**

<http://www.oasis-open.org/committees/download.php/18158/EML%20v4.0%20-%20OASIS%20Standard.zip>

**Latest Version:**

<http://docs.oasis-open.org/election/eml/v5.0/EML-Process-Data-Requirements-v5.0.doc>  
<http://docs.oasis-open.org/election/eml/v5.0/EML-Process-Data-Requirements-v5.0.html>  
<http://docs.oasis-open.org/election/eml/v5.0/EML-Process-Data-Requirements-v5.0.pdf>  
<http://docs.oasis-open.org/election/eml/v5.0/EML-v5.0-cd01.zip>

**Technical Committee:**

OASIS Election and Voter Services TC

**Chair:**

John Borrás

**Editor:**

John Borrás

**Related work:**

This specification supercedes:

- Election Markup Language (EML) v4.0

See also:

- [EML Schema Descriptions](#)
- [EML Data Dictionary](#)

**Declared XML Namespace:**

urn:oasis:names:tc:evs:schema:eml

**Abstract:**

This document describes the background and purpose of the Election Markup Language, the electoral processes from which it derives its structure and the security and audit mechanisms it is designed to support.

The relating document entitled 'EML v5.0 Schema Descriptions' lists the schemas and schema descriptions to be used in conjunction with this specification.

**Status:**

This document was last revised or approved by the Election and Voter Services Technical Committee on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/election/>

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/election/ipr.php>)

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/election/>.

---

## Notices

Copyright © OASIS® 1993–2007. All Rights Reserved. OASIS trademark, IPR and other policies apply.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

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 section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, 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 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

---

# Table of Contents

1	Executive Summary.....	6
1.1	Terminology .....	7
1.2	Normative References .....	7
1.3	Non-Normative References .....	7
2	Introduction.....	8
2.1	Business Drivers.....	8
2.2	Technical Drivers .....	8
2.3	The E&VS Committee.....	8
2.4	Challenge and Scope .....	9
2.5	Documentation Set .....	10
2.6	Conformance .....	11
2.7	Voting Terminology.....	11
3	High-Level Election Process .....	13
3.1	Figure 2A High Level Model – Human View.....	14
3.2	Figure 2B High Level Model – Technical View.....	15
3.3	Outline.....	16
3.4	Process Descriptions .....	16
3.4.1	The Candidate Nomination Process .....	16
3.4.2	The Options Nomination Process .....	18
3.4.3	The Voter Registration .....	19
3.4.4	The Voting Process .....	20
3.4.5	The Vote Reporting Process .....	22
3.4.6	The Auditing System .....	23
3.5	Data Requirements.....	24
4	Security Considerations .....	25
4.1	Basic Security Requirements.....	25
4.1.1	Authentication.....	25
4.1.2	Privacy/Confidentiality .....	26
4.1.3	Integrity.....	26
4.1.4	Non-Repudiation .....	26
4.2	Terms.....	27
4.3	Specific Security Requirements.....	27
4.4	Security Architecture.....	28
4.4.1	Voter identification and registration.....	28
4.4.2	Right to vote authentication.....	29
4.4.3	Protecting exchanges with remote voters .....	29
4.4.4	Validation right to vote and contest vote sealing.....	30
4.4.5	Vote Confidentiality .....	30
4.4.6	Candidate List integrity.....	30
4.4.7	Vote counting accuracy.....	30
4.4.8	Voting System Security .....	31
4.5	Remote voting security concerns .....	31
5	Schema Outline.....	33

5.1 Structure .....	33
5.2 IDs.....	33
5.3 Displaying Messages.....	33
6 Schema Descriptions .....	37
A. Acknowledgements .....	38
B.....	39
B.1 Internet Voting Security Concerns .....	39
B.2 The Timestamp Schema .....	42
B.3 W3C XML Digital Signature.....	45
C. Revision History.....	47

---

# 1 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 systems involved in the election process to interact. The overall effort attempts to address the challenges of developing a standard that is:

- **Multinational:** Our aim is to have these standards adopted globally.
- **Flexible:** Effective across the different voting regimes (e.g. proportional representation or 'first past the post') and voting channels (e.g. Internet, SMS, postal or traditional paper ballot).
- **Multilingual:** Flexible enough to accommodate the various languages and dialects and vocabularies.
- **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 is 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
- Referendum Options Nomination, Response to Nomination and Approved Options Lists
- Voter Registration information, including eligible voter lists
- Various communications between voters and election officials, such as polling information, election notices, etc.
- 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
- EML is flexible enough to be used for elections and referendums that are primarily paper-based or that are fully e-enabled.

## Overview of the 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 2** 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 3** 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.

44 **Section 4** presents a discussion of the some of the common security requirements faced in different  
45 election scenarios, a possible security model, and the mechanisms that are available in the EML  
46 specifications to help address those requirements. The scope of election security, integrity and audit  
47 included in these interface descriptions and the related discussions are intended to cover security issues  
48 pertinent only to the standardised interfaces and not to the internal security requirements within the  
49 various components of election systems.

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

55 **Section 5** provides an overview of the approach that has been taken to creating the XML schemas.

56 **Section 6** provides information as to the location of the descriptions of the schemas developed to date.

57 **Appendices** provide information on internet voting security concerns, TimeStamp schema, W3C Digital  
58 Signature, Acknowledgements and a revision history.

59

## 60 1.1 Terminology

61 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD  
62 NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described  
63 in [RFC2119].

## 64 1.2 Normative References

65 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
66 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

## 67 1.3 Non-Normative References

68 **xNAL** eXtensible Name and Address (xNAL) Specifications and Description Document  
69 (v2.0) Customer Information Quality Technical Committee OASIS July 2002  
70 [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=ciq](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq)

71 **UK's APD** Address and Personal Details Fragment v1.1 Technology Policy Team, e-  
72 Government Unit, Cabinet Office UK, 1 March 2002  
73 [http://www.govtalk.gov.uk/interoperability/draftschema\\_schema.asp?schemaid=92](http://www.govtalk.gov.uk/interoperability/draftschema_schema.asp?schemaid=92)

74 **XML** Extensible Markup Language (XML) 1.0 (Third Edition) Tim Bray et al, Worldwide  
75 Web Consortium, 4 February 2004 <http://www.w3.org/TR/REC-xml>

76 **XML-DSig** XML-Signature Syntax and Processing Donald Eastlake et al, Worldwide Web  
77 Consortium, 12 February 2002 <http://www.w3.org/TR/xmlsig-core/>

78 **VoiceXML** Voice Extensible Markup Language (VoiceXML) Version 2.0 Scott McGlashan et al  
79 Worldwide Web Consortium 16 March 2004 <http://www.w3.org/TR/voicexml20>

80

---

## 81 2 Introduction

### 82 2.1 Business Drivers

83 Voting is one of the most critical features in our democratic process. In addition to providing for the  
84 orderly transfer of power, it also cements the citizen's trust and confidence in an organization or  
85 government when it operates efficiently. In the past, changes in the election process have proceeded  
86 deliberately and judiciously, often entailing lengthy debates over even the most minute detail. These  
87 changes have been approached with caution because discrepancies with the election system threaten  
88 the very principles that make our society democratic.

89 Times are changing. Society is becoming more and more web oriented and citizens, used to the high  
90 degree of flexibility in the services provided by the private sector and in the Internet in particular, are now  
91 beginning to set demanding standards for the delivery of services by governments using modern  
92 electronic delivery methods.

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

96 The implementation of electronic voting would allow increased access to the voting process for millions of  
97 potential voters. Higher levels of voter participation will lend greater legitimacy to the electoral process  
98 and should help to reverse the trend towards voter apathy that is fast becoming a feature of many  
99 democracies. However, it has to be recognized that the use of technology will not by itself correct this  
100 trend. Greater engagement of voters throughout the whole democratic process is also required.

101 However, it is recognized that more traditional voting methods will exist for some time to come, so a  
102 means is needed to make these more efficient and integrate them with electronic methods.

### 103 2.2 Technical Drivers

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

108 The introduction of open standards for election solutions is intended to enable election officials around the  
109 world to build upon existing infrastructure investments to evolve their systems as new technologies  
110 emerge. This will simplify the election process in a way that was never possible before. Open election  
111 standards will aim to instill confidence in the democratic process among citizens and government leaders  
112 alike, particularly within emerging democracies where the responsible implementation of the new  
113 technology is critical.

### 114 2.3 The E&VS Committee

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

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

123 The Committee's mission statement is:

124 *"Develop a standard for the structured interchange of data among hardware, software, and service*  
125 *providers who engage in any aspect of providing election or voter services to public or private*

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

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

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

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

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

- 147 • Multinational – our aim is to have these standards adopted globally
- 148 • Effective across the different voting regimes – for example, proportional representation or 'first past  
149 the post', preferential voting, additional member system
- 150 • Multilingual – our standards will need to be flexible enough to accommodate the various languages  
151 and dialects and vocabularies
- 152 • Adaptable – our aim is to provide a specification that is resilient enough to support elections in both  
153 the private and public sectors
- 154 • Secure – the standards must provide security that protects election data and detects any attempt to  
155 corrupt it.

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

## 158 **2.4 Challenge and Scope**

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

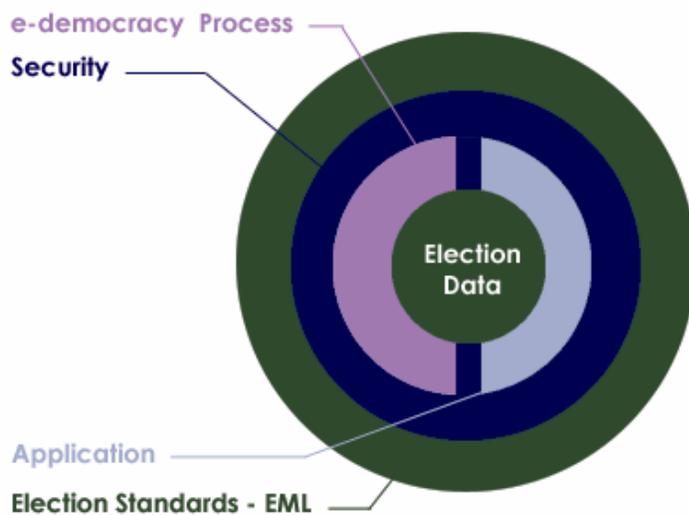
164 These processes are illustrative, covering the vast majority of election types and forming a basis for  
165 defining the Election Markup Language itself. EML has been designed such that elections that do not  
166 follow this process model should still be able to use EML as a basis for the exchange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

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

174 The security requirement for the election system design, implementation or evaluation must be placed  
175 within the context of the vulnerabilities and threats analysis of a particular election scenario. As such the  
176 references to security within EML are not to be taken as comprehensive requirements for all election  
177 systems in all election scenarios, nor as recommendations of sufficiency of approach when addressing all  
178 the security aspects of election system design, implementation or evaluation. In fact, the data security  
179 mechanisms described in this document are all optional, enabling compliance with EML without regard for  
180 system security at all. A complementary document may be defined for a specific election scenario, which  
181 refines the security issues defined in this document.

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

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



191  
192 **Figure 1A: Relationship overview**

## 193 2.5 Documentation Set

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

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

202 The EML specification is being used in a number of pilots to test it's effectiveness across a number of  
203 different international jurisdictions. The committee document set will include:

- 204 • **Voting Processes:** A general and global study of the electoral process. This introduces the transition  
205 from a complete human process by defining the data structure to be exchanged and where they are  
206 needed.
- 207 • **Data Requirements:** A data dictionary defining the data used in the processes and required to be  
208 handled by the XML schemas.

- 209 • **EML Specifications:** This consists of a library of XML schemas used in EML. The XML schemas  
210 define the formal structures of the election data that needs to be exchanged.
- 211 • **Report on Alternative methods of EML Localisation:** EML provides a set of constraints common to  
212 most types of elections worldwide. Each specific election type will require additional constraints, for  
213 example, to enforce the use of a seal or to ensure that a cast vote is anonymous. This document  
214 describes alternative mechanisms for expressing these constraints and recommends the use of  
215 schemas using the Schematron language to supplement the EML schemas for this purpose.

## 216 2.6 Conformance

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

Schema	Accept	Generate
EML110	v4.0, v3.0	
EML310	v4.0, v3.0	
EML330		v4.0
EML340		v4.0
EML350		v4.0
EML360		v4.0

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

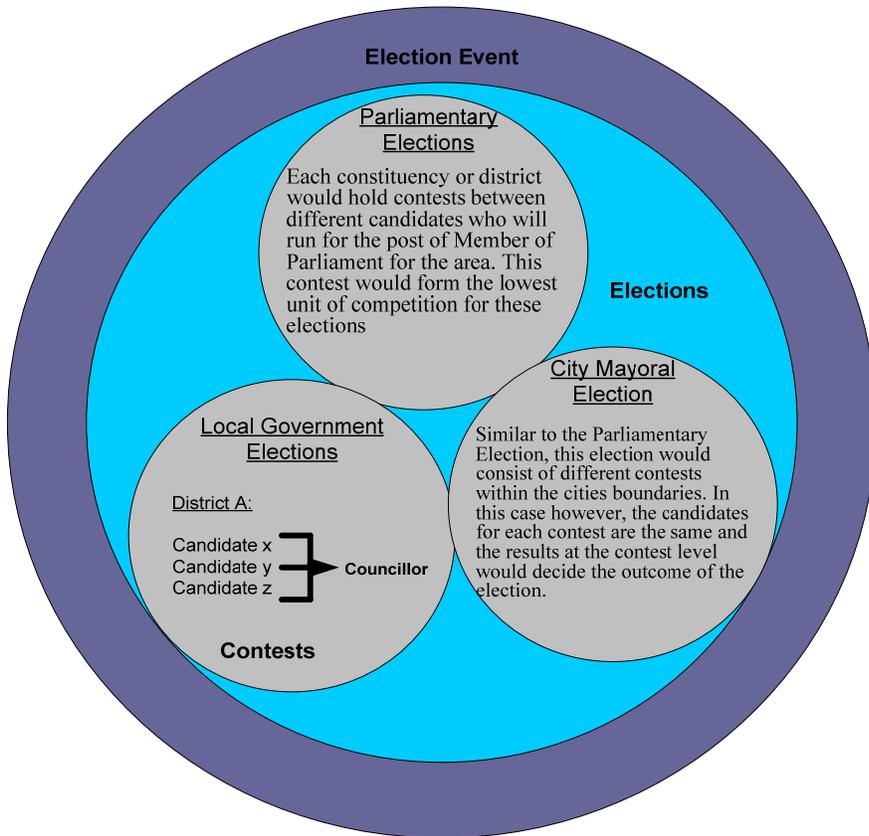
## 224 2.7 Voting Terminology

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

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

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

233 In practice however, electoral authorities would often run a number of different elections during a defined  
234 time period. This phenomenon is captured in our terminology as an Election Event. Figure 1B uses a  
235 British context to describe our approach in general terms.

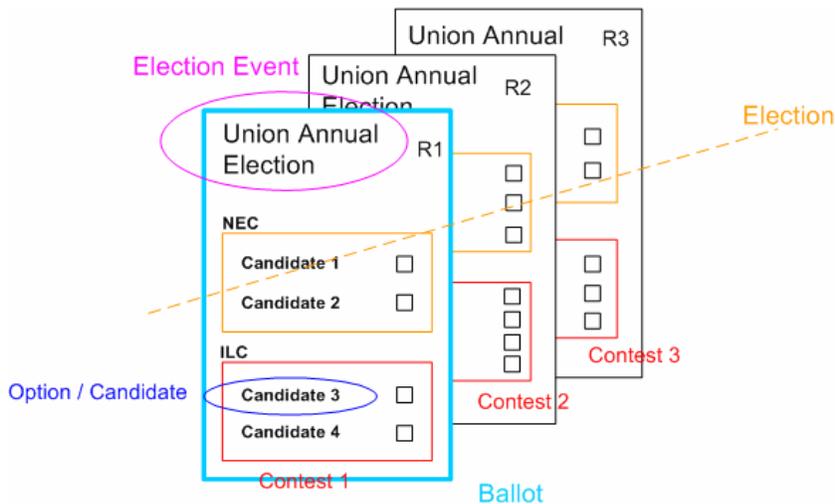


236

237 **Figure 1B: The Election Hierarchy**

238 In Figure 1C, there is an Election Event called the 'Union Annual Election'. This comprises two Elections,  
 239 one for the National Executive Committee (NEC) and one for the International Liaison Committee (ILC).  
 240 Three positions are being selected for each committee; as a result, each Election is made up of three  
 241 Contests. In region 1 (R1), the Contest for each Election has two Candidates.

242 Figure 1C shows the three Ballots (one for each region). The Ballot is personal to the voter and presents  
 243 the Candidates available to that voter. It also allows choices to be made. During the election exercise,  
 244 each voter in region 1 (R1) receives only the region 1 ballot. This ballot will contain the Candidates for the  
 245 R1 contest for each of the two Elections.



246

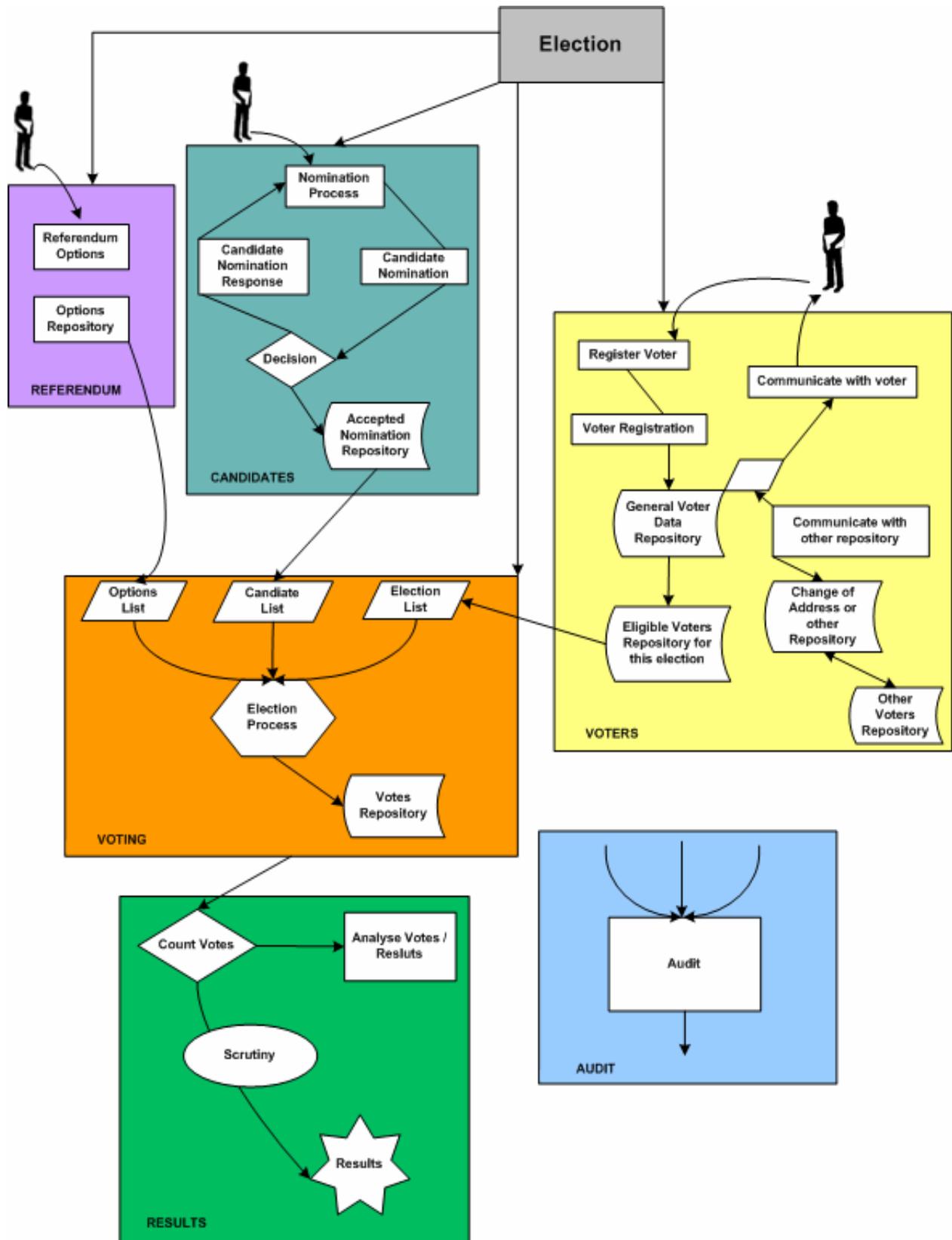
247 **Figure 1C: Union Annual Election**

---

248 **3 High-Level Election Process**

249 Section 3 describes two complementary high level process models of an election exercise, based on the  
250 human and technical views of the processes involved. It is intended to identify all the generic steps  
251 involved in the process and all the areas where data is to be exchanged highlight all the areas where data  
252 is to be exchanged.

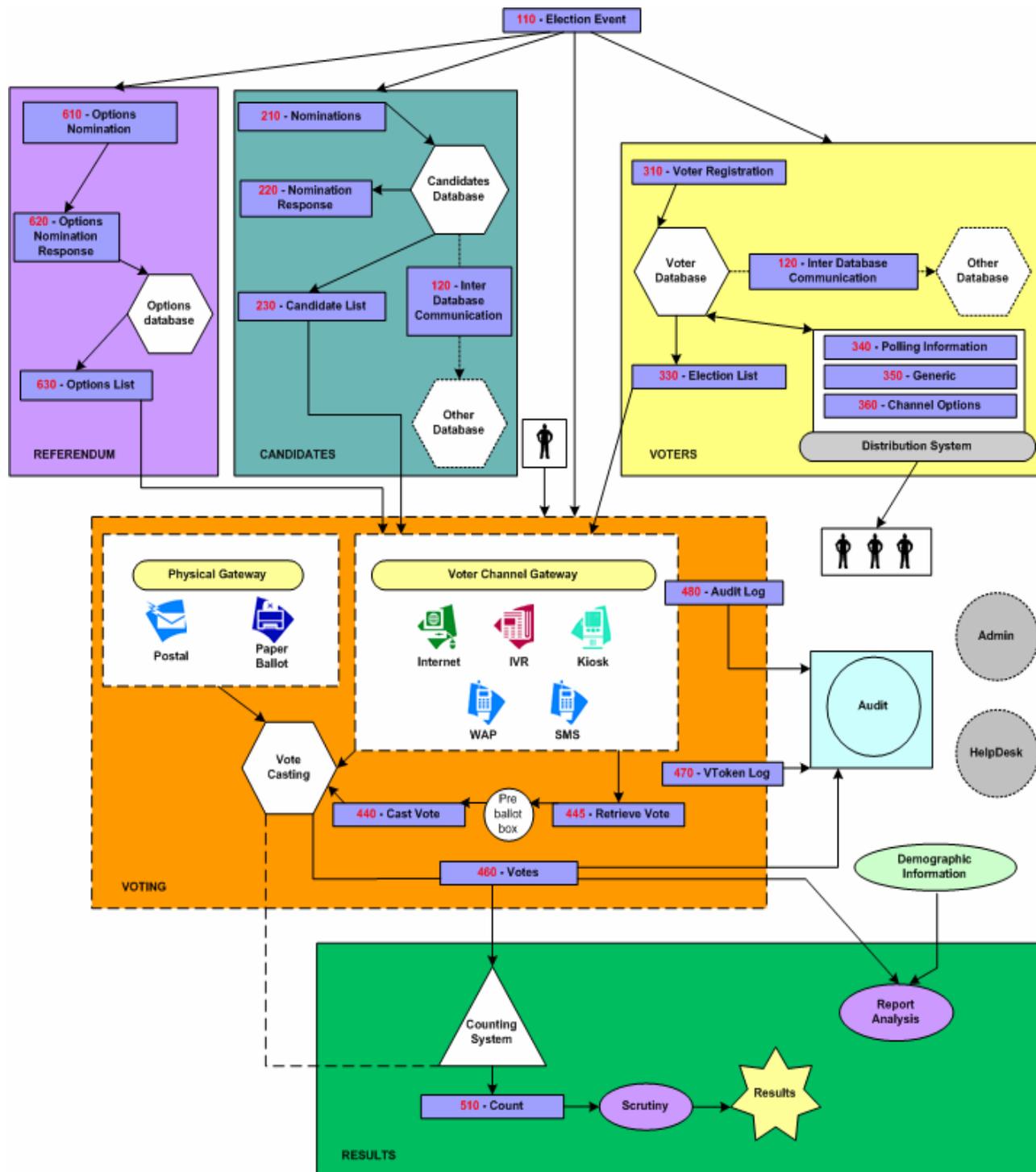
253 3.1 Figure 2A High Level Model – Human View



254

255 3.2 Figure 2B High Level Model – Technical View

256



257

258

259

## 260 **3.3 Outline**

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

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

- 267 • Pre election
- 268 • Election (100)
- 269 • Candidates (200)
- 270 • Options (600)
- 271 • Voters (300)
- 272 • Election
- 273 • Voting (400)
- 274 • Post election
- 275 • Results (500)
- 276 • Audit
- 277 • Analysis

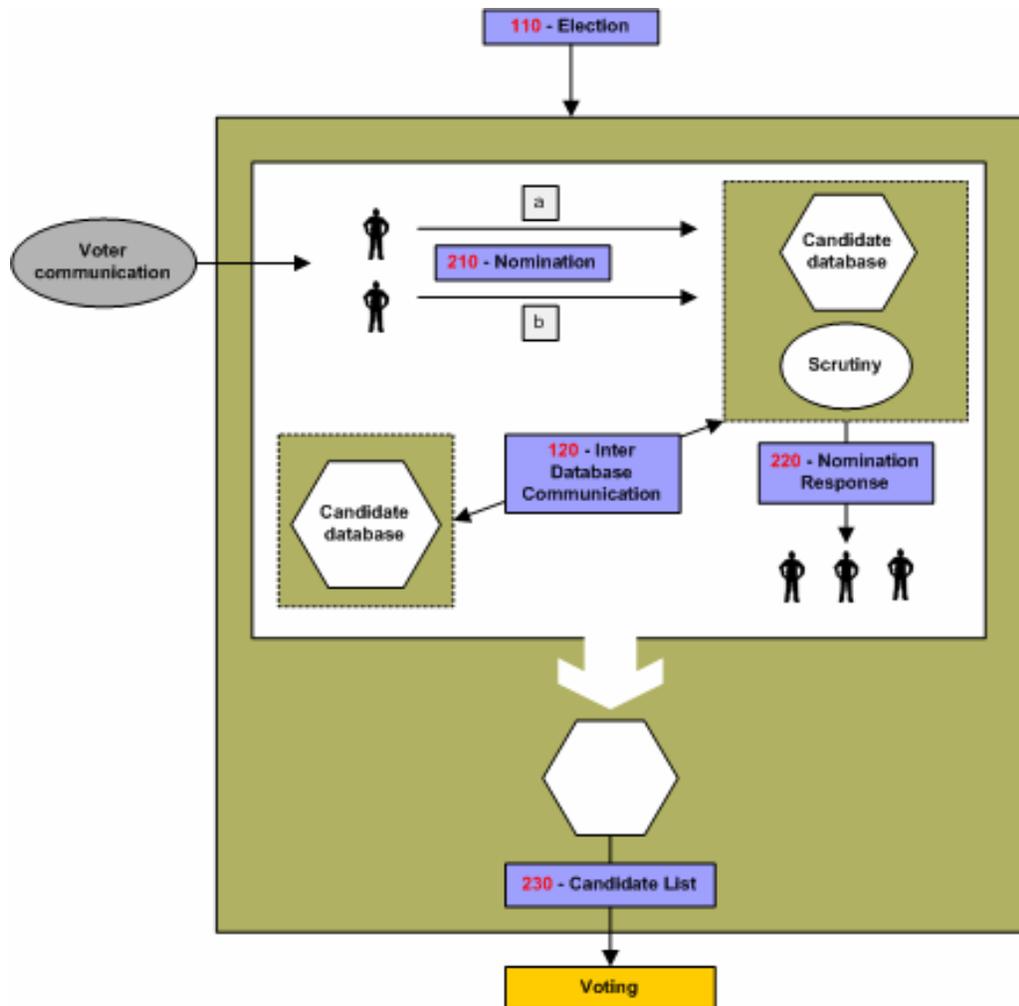
278 Some functions belong to the whole process and not to a specific part:

- 279 • Administration Interface
- 280 • Help Desk

## 281 **3.4 Process Descriptions**

### 282 **3.4.1 The Candidate Nomination Process**

283 This is the process of approving nominees as eligible candidates for certain positions in an election. A  
284 candidate in this context can be a named individual or a party.



285

286 **Figure 2C: The Candidate Nomination Process**

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

- 290
- 291 • Voter Communications [350-Generic] declaring the opening of nominations will be used to reach the population eligible to nominate candidates for a position x in an election y.
  - 292 • Interested parties will respond in the proper way satisfying the rules of nomination for this election
  - 293 with the objective of becoming running candidates. The response message conforms to schema 210.
  - 294 • A nomination for an individual candidate can be achieved in one of two ways:
  - 295 • A Nominee will reply by attaching to his nomination a list of x number of endorsers with their
  - 296 signature.
  - 297 • Each endorser will send a message specifying Mr. X as his or her nominee for the position in
  - 298 question. Mr X will signal his agreement to stand.

299 Note that nomination and the candidate's agreement to stand might be combined in a single message or  
 300 sent as two messages, each conforming to schema 210.

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

- 304
- 305 • Pay fees,
  - Have x number of endorsers,

- 306 • Be of a certain age,
- 307 • Be a citizen more than x number of years,
- 308 • Not stand for election in more than one contest at a time,
- 309 • Etc.

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

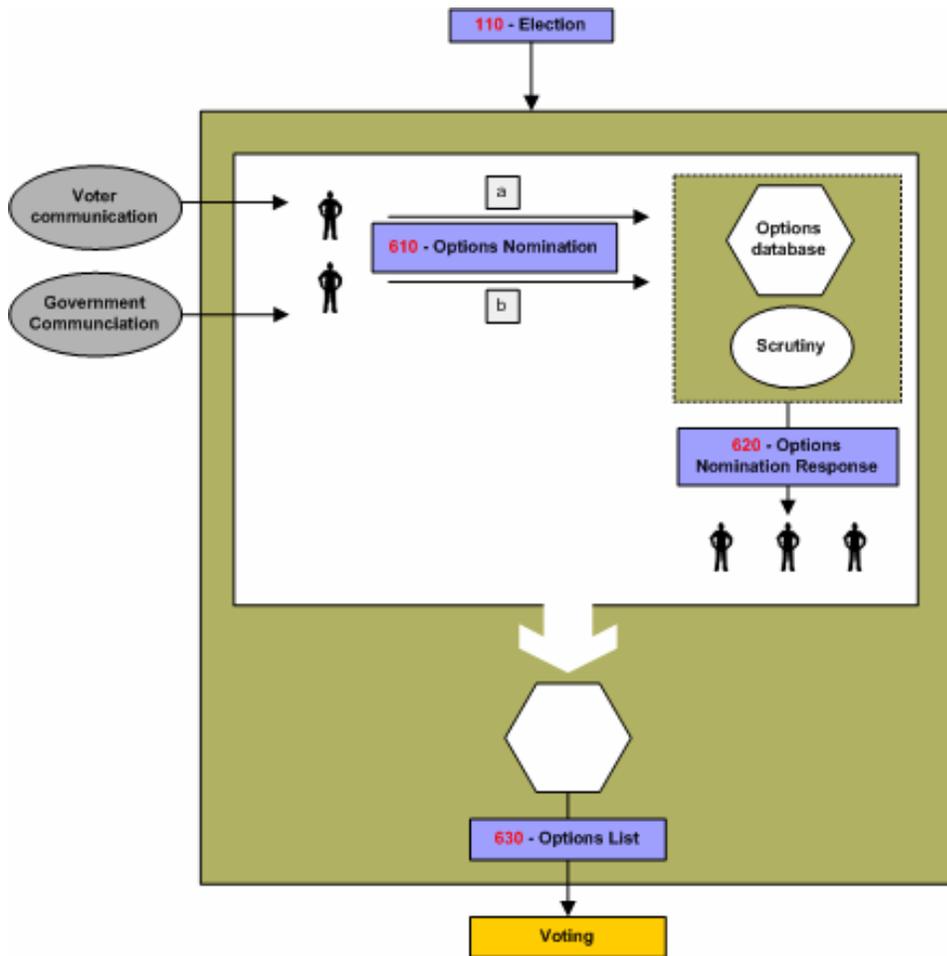
312 Schema 120 allows election officials to enquire of other jurisdictions whether a particular candidate is  
 313 standing in more than one contest.

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

315 The outcome of this process is a list of accepted candidates that will be communicated using a message  
 316 conforming to schema 230. It will be used to construct the list of candidates for each contest.

### 317 3.4.2 The Options Nomination Process

318 This is the process of approving the options to be presented to voters in a referendum. The options can  
 319 be a straight choice, e.g. YES or NO, to a single question, or can be more complex involving choices to a  
 320 number of questions and/or preferences of choice.



321  
 322 **Figure 2D: Referendum Options Nomination Process**

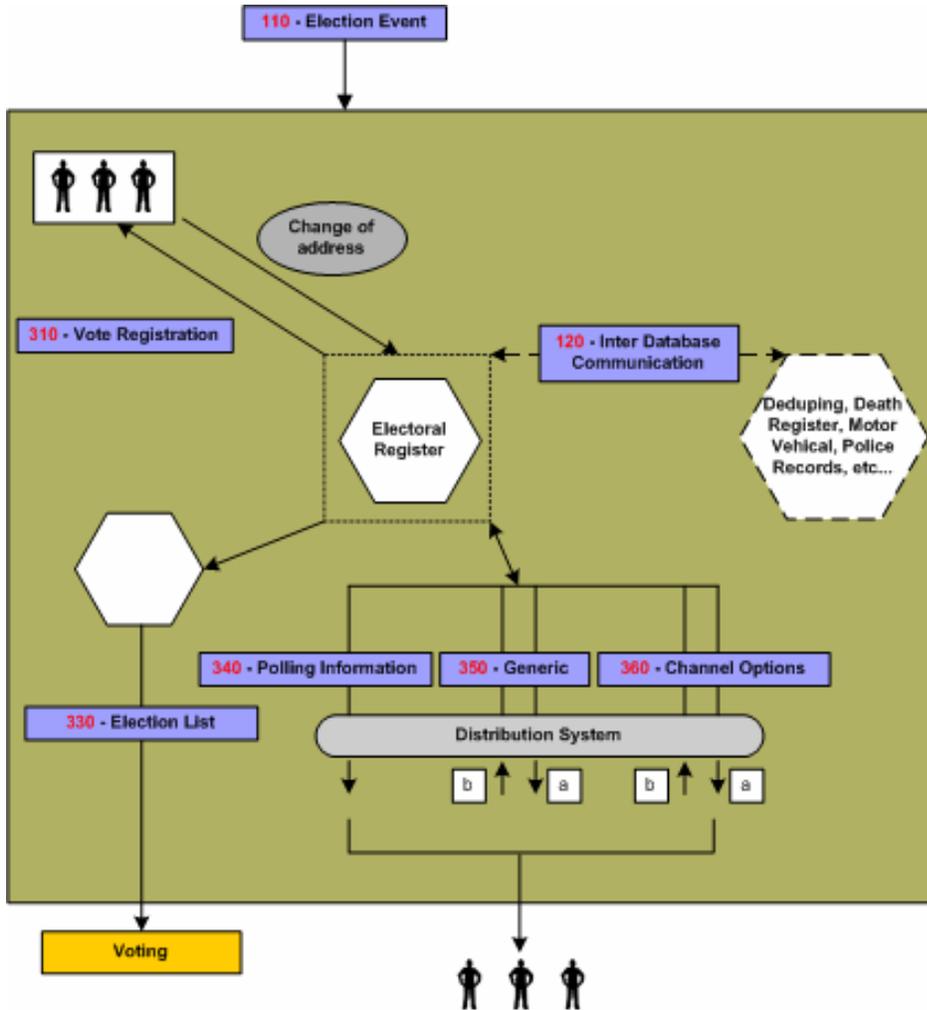
323 The nomination can be received in a number of ways including direct from government institutions or from  
 324 citizens or businesses, and schema 610 handles the receipt of nominations.

325 Nominees may be notified of the result of any scrutiny of their nomination using a message conforming to  
 326 schema 620.

327 The outcome of this process is a list of accepted options that will be communicated using a message  
328 conforming to schema 630. It will be used to construct the list of referendum questions for each contest.

### 329 3.4.3 The Voter Registration

330 This is the process of recording a person's entitlement to vote on a voter registration system. A key part of  
331 this process is the identification of the person.



332  
333 **Figure 2E: Voter Registration**

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

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

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

345 At a certain date, a subset of the voters' database is fixed from which the election list is generated.  
346 Schemas contain some subset of the eligible voters, perhaps grouped by polling district or voting channel.

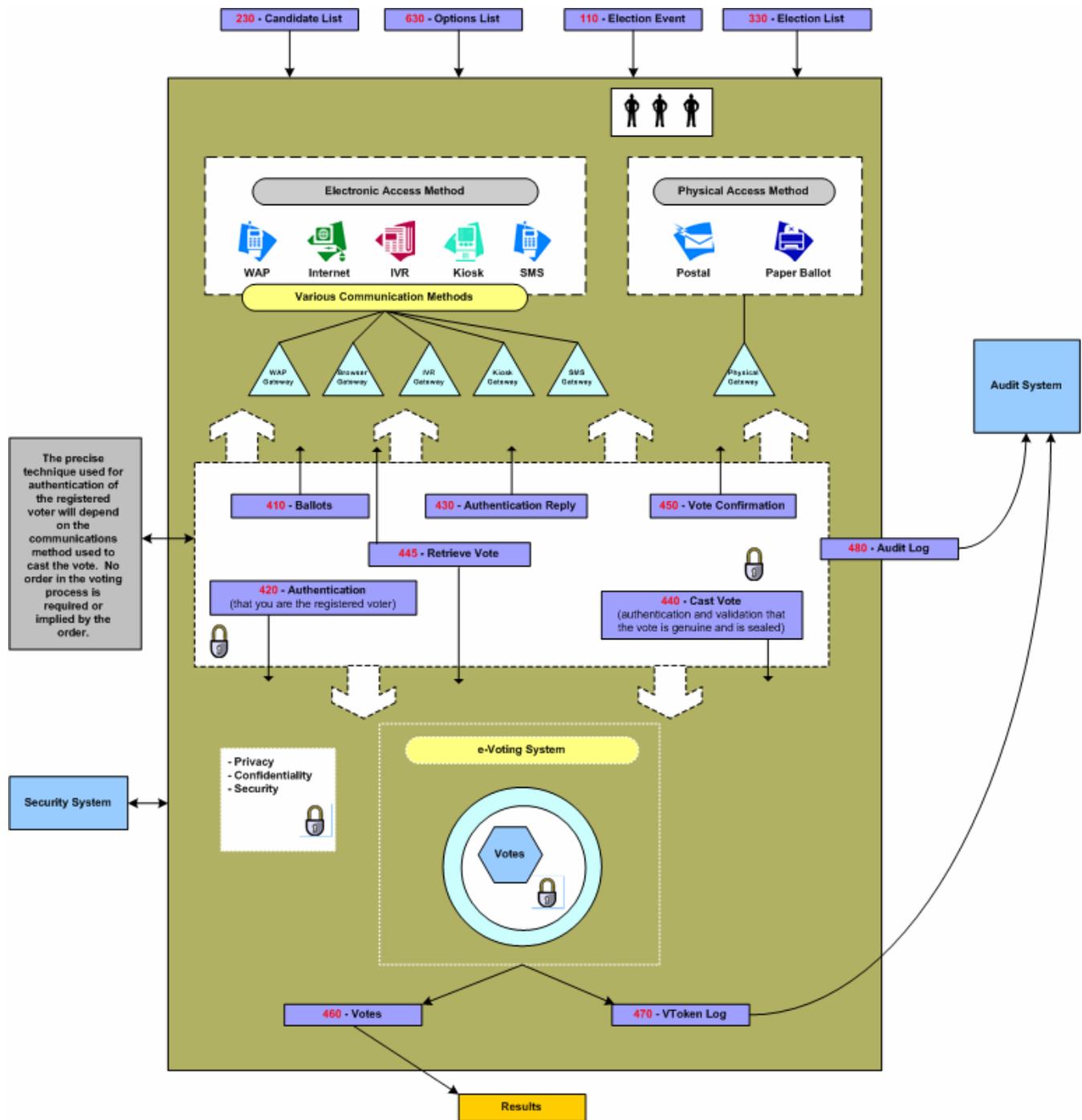
347 It is here that we introduce the concept of voter communications. Under this category we divided them  
348 into three possible types of communications:

- 349 • Channel options
- 350 • Polling Information
- 351 • Generic.

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

#### 354 **3.4.4 The Voting Process**

355 This is the process that involves the authentication of the voter and the casting of an individual vote.



356  
 357 **Figure 2F: The Voting Process**

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

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

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

367 When a pre-ballot box is required in a scenario, schema 445 can be used to retrieve and amend votes  
 368 before they are counted.

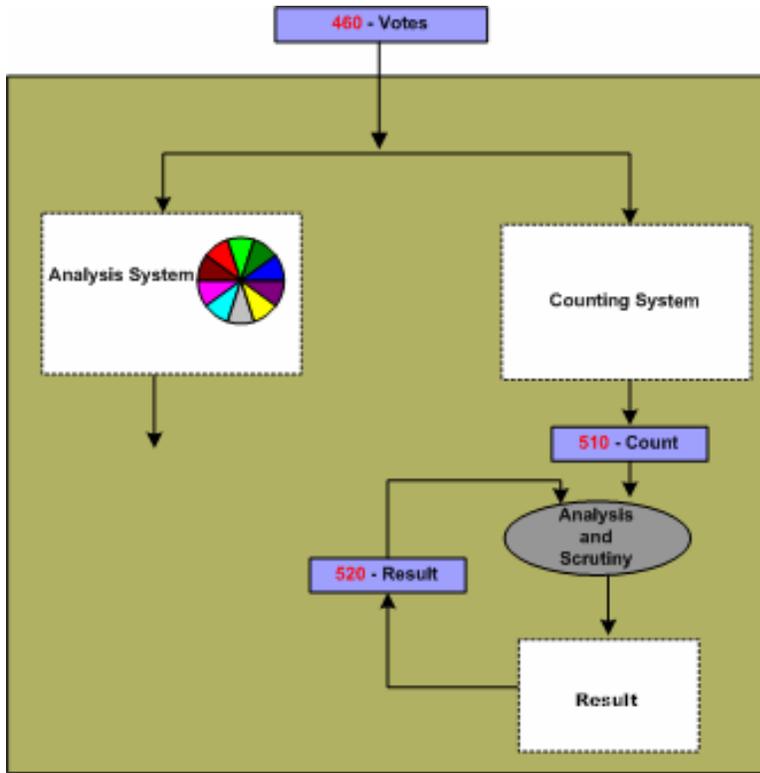
369 Where a voter's right to vote in any particular contest needs to be determined, this is defined by the  
 370 parameters of his VToken. See Section 4 for more information on security and the VToken.

371 In some scenarios the right to vote may need to be qualified. This may occur if the voter's right to vote is  
 372 challenged or if the voter is given the temporary right to vote. In this case the vote needs to be cast by a  
 373 voter with a Qualified VToken. The reason for the qualification shall always be present in a Qualified  
 374 VToken and the qualification may need to be investigated before the vote is counted as legitimate. The  
 375 VToken and Qualified VToken are part of schemas 420, 440, 450, 460 and 470.

376 To create balloting information, input data is needed about the election, the options/candidates available  
 377 and the eligible voters; see schemas 230, 110 and 120 for exchanging such information between e-  
 378 systems.

379 **3.4.5 The Vote Reporting Process**

380 Two of the post election items are the Final or Interim Result and the Audit Report. Audit is discussed in  
 381 3.4.6.



382  
 383 **Figure 2G: The Vote Reporting Process**

384 The voting system should communicate a bulk of data representing the votes to the counting system or  
 385 the analysis system-using schema 460. The count of these, which is the compilation of the 460, is to be  
 386 communicated by the schema 510.

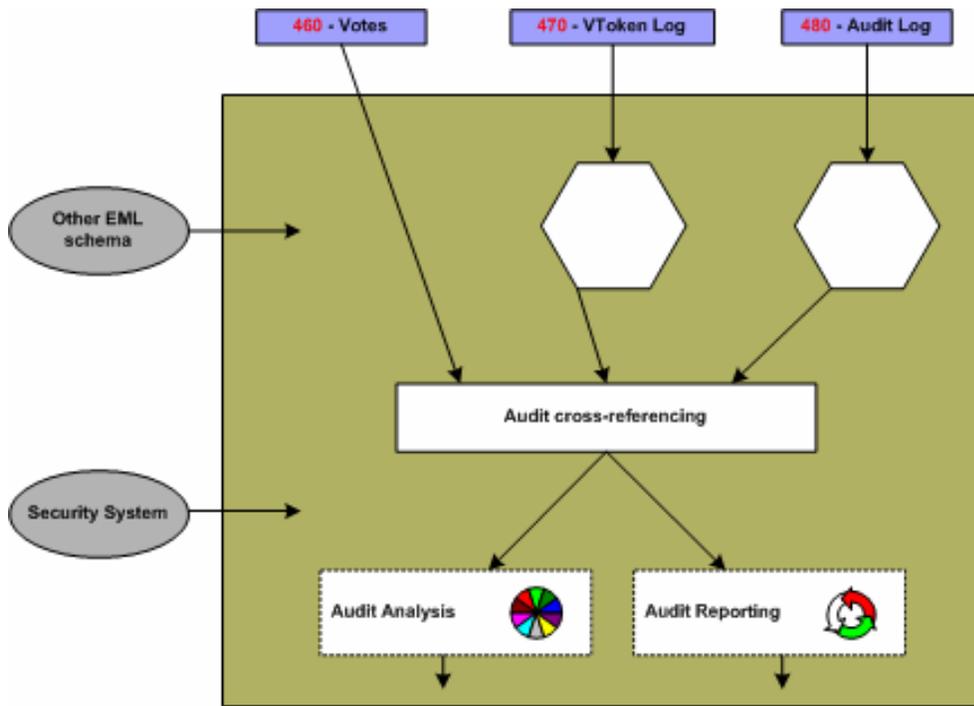
387 Recount can be very simply accommodated by a re-run of the schema 460, on the same or another  
 388 counting system.

389 Some voting methods, such as the additional member system (AMS), combine the result of one election  
 390 with the votes of another to create a result. For an election run under the AMS, the results of the 'first past  
 391 the post' (FPP) election can be communicated using a message conforming to schema 520. This schema  
 392 can only be used for communicating the results of elections using simple voting methods such as FPP,  
 393 and is not intended as a general purpose results schema.

394 The votes schema 460 also feeds into an analysis system, which is used to provide for demographic or  
 395 other types of election reports. The output of the analysis system is outside the scope of this document.  
 396 Schemas 510 and 520 allow for Simulation and Extrapolation of final or interim Counts and Results.  
 397 Simulation being the facility to forecast the result of a contest based on the result of another contest.  
 398 Extrapolation is the facility to forecast the final result of a contest based on the count so far.  
 399 Further schemas may be developed that make use of the Votes and Count schemas. For example  
 400 schemas for messages that report election results to the media.

### 401 3.4.6 The Auditing System

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



405  
 406 **Figure 2H: Auditing System**

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

409 Schemas 460, 470, 480 from the voting process provide input data to the audit process. Depending on  
 410 the audit requirements additional data from other processes may be required. In particular, the security  
 411 process may provide additional data about all the issued VTokens and Qualified VTokens (see Figure 3A:  
 412 Voting system security).

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

- 416 • Eligible voters
- 417 • Issued VTokens or Qualified VTokens.

418 The audit process can collate the total number of VTokens and Qualified VTokens provided by the  
 419 security system with the total number reported by the voting system using schema 460 and 470.

420 The security system and sealing mechanism should be implemented so that trust can be placed in the  
 421 seal and hence the sealed data. This implies that the seal should be performed as close to the user  
 422 submission of the vote as technically possible. The count of the spoiled and unspoiled votes from 460 can

423 then be cross-checked against the count of the number of trusted seals from 480. This correlation  
424 confirms that the total number of votes presented by the output of the e-voting system in 460 is consistent  
425 with the total number of submitted votes with seals.

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

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

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

438 There is also the requirement for the election officer to be provided with a mechanism that allows for  
439 multiple observers to witness all the voting process. How this is achieved is dependant on the  
440 implementation of the system and procedures adopted. However, the seals and channel information  
441 using schema 480 provide the ability to observe voting inputs per channel while voting is in progress  
442 without revealing the vote itself or the voter's identity. The final count of the seals can then be used to  
443 cross check the totals of the final result as described above.

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

### 449 **3.5 Data Requirements**

450 The data used in all the above processes are defined in 'EML v5.0 Data Dictionary'.

---

## 451 **4 Security Considerations**

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

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

### 461 **4.1 Basic Security Requirements**

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

- 465 • Security considerations of e-voting systems include:
- 466 • Authentication
- 467 • Privacy/Confidentiality
- 468 • Integrity
- 469 • Non-repudiation

#### 470 **4.1.1 Authentication**

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

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

- 474 • Checking a claim of identity
- 475 • Checking a right to vote.

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

479 In other scenarios the voter’s identity must remain private and must not be revealed by a ballot. In which  
480 case some systems may provide a clear separation between checking of the claim of identity, which may  
481 be done some time before the ballot takes place, from checking the right to vote at the time of the vote is  
482 cast. Alternatively, other mechanism may be used to ensure the privacy of the voter’s identity on cast  
483 votes (i.e. by anonymizing the ballot).

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

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

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

493 Authentication of the right to vote by itself does not reveal a voter's identity, but does verify he has a  
494 legitimate right to vote (e.g. the VToken data provides authentication of the right to vote but has  
495 anonymous properties as to the identification of the person voting).

496 An voter's identity and the right to vote are both validated (i.e. the VToken data has both 'voter  
497 identification' and 'right to vote' authentication properties) and then the cast votes are clearly separated  
498 from the identity of the voter (i.e. the voters identification occurs before the ballot is 'anonymized')

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

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

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

### 507 **4.1.2 Privacy/Confidentiality**

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

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

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

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

### 523 **4.1.3 Integrity**

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

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

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

### 536 **4.1.4 Non-Repudiation**

537 Non-repudiation is a derivative of the identification problem. Identification in e-voting requires that the  
538 system provide some level of assurance that the persons representing themselves as valid participants  
539 (voters, election workers, etc.) are, in fact, who they claim to be. Non-repudiation requires that the system  
540 provides some level of assurance that the identified participant is not able to successfully assert that the

541 actions attributed to them via the identification mechanism were, in fact, performed by someone else. The  
542 two requirements are related in that a system with a perfect identification mechanism and undisputable  
543 proof of all actions would leave no room for successful repudiation claims.

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

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

## 561 **4.2 Terms**

562 The following security terms are used in this document:

- 563 • Identity Authentication: the means by which a voter registration system checks the validity of the  
564 claimed identity.
- 565 • Right to vote authentication: the means by which the voting system checks the validity of a voter’s  
566 right to vote.
- 567 • VToken: the means by which a voter proves to an e-voting system that he/she has the right to vote in  
568 a contest.
- 569 • VToken Qualified: the means by which a VToken can be qualified. The reason for the qualification is  
570 always appended to a VToken that is qualified. For example, a qualified VToken may be issued to a  
571 challenged voter.
- 572 • Vote sealing: the means by which the integrity of voting data (ballot choices, vote cast against a given  
573 VToken) can be protected (e.g. using a digital signature or other authentication code) so that it can be  
574 proved that a voter’s authentication and one or more votes are related.

## 575 **4.3 Specific Security Requirements**

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

- 577 • Only legitimate voters are allowed to vote (i.e. voters must be authenticated as having the right to  
578 cast a vote)
- 579 • Only one set of choices is allowed per voter, per contest
- 580 • The vote cannot be altered from the voter’s intention
- 581 • The vote may not be observed until the proper time
- 582 • The voting system must be accountable and auditable
- 583 • Information used to authenticate the voter or his/her right to vote should be protected against misuse  
584 (e.g. passwords should be protected from copying)
- 585 • Voter privacy must be maintained according to the laws of the election jurisdiction. (Legal  
586 requirements of public elections in various countries conflict. Some countries require that the vote  
587 cannot be tracked back to the voter’s identity, while others mandate that it must be possible to track  
588 every vote to a legitimate voter’s identity)

- 589 • The casting options available to the voter must be genuine
- 590 • Proof that all genuine votes have been accurately counted.
- 591 There are some specific complications that arise with respect to security and electronic voting that
- 592 include:
- 593 • Several technologies may be employed in the voting environment
- 594 • The voting environment may be made up of systems from multiple vendors
- 595 • A voter may have the option to vote through alternative delivery channels (i.e. physically presenting
- 596 themselves at a polling station, by post, by electronic means)
- 597 • The voting systems need to be able to meet various national legal requirements and local voting rules
- 598 for both private and public elections
- 599 • Need to verify that all votes are recorded properly without having access to the original input
- 600 • The mechanism used for voter authentication may vary depending on legal requirements of the
- 601 contest, the voter registration and the e-voting systems for private and public elections
- 602 • The user may be voting from an insecure environment (e.g. a PC with no anti-virus checking or user
- 603 access controls).
- 604 In addition, the objectives of security architectures for electronic voting systems should include:
- 605 • Being open
- 606 • Not restricting the authentication mechanisms provided by e-voting systems
- 607 • Specifying the security characteristic required of an implementation, allowing for freedom in its
- 608 precise implementation.
- 609 • Providing the means to exercise security isolation and controls at interfaces between various election
- 610 processes, thereby providing the ability to implement isolated trusted logic processes to meet
- 611 dedicated functions of an election service. Process security isolation ensures that one voting sub-
- 612 process does not inadvertently effect another voting sub-process thereby undermining the whole
- 613 voting system.

## 614 **4.4 Security Architecture**

615 The architecture proposed here is designed to meet the security requirements and objectives detailed

616 above, allowing for the security complications of e-voting systems listed.

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

- 618 • Voter identification and registration
- 619 • Right to vote authentication
- 620 • Protecting exchanges with remote voters
- 621 • Validating Right to Vote and contest vote sealing
- 622 • Vote confidentiality.
- 623 • Candidate list Integrity
- 624 • Vote counting accuracy
- 625 • Voting system security controls.

### 626 **4.4.1 Voter identification and registration**

627 The Voter identification and registration is used to identify an entity (e.g. person) for the purpose of

628 registering the person has a right to vote in one or more contests, thus identifying legitimate voters. The

629 security characteristics for voter identification are to be able to authenticate the identity of the legal person

630 allowed to vote in a contest and to authenticate each person's voting rights. The precise method of voter

631 identification is not defined here, as it will be specific to particular voting environments, and designed to

632 meet specific legal requirements, private or public election and contest rules. The voter registration

633 system may interact with the e-voting system and other systems to define how to authenticate a voter for  
634 a particular contest.

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

#### 642 **4.4.2 Right to vote authentication**

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

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

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

659 The security characteristic required of the VToken may also vary depending on legal requirements of a  
660 country or electoral rules used in a particular contest. Also, the threats to misuse of VTokens will depend  
661 to a large degree on the voting channels used (e.g. physical presence at voting station, Internet, mobile  
662 phone). Bearing this in mind the XML schema of the VToken components must allow for various data  
663 types of authentication information to be contained within it.

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

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

#### 673 **4.4.3 Protecting exchanges with remote voters**

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

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

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

#### 685 **4.4.4 Validation right to vote and contest vote sealing**

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

- 691 • The vote cannot be altered from the voter's intention
- 692 • The voting system is accountable and auditable.

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

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

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

#### 706 **4.4.5 Vote Confidentiality**

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

#### 711 **4.4.6 Candidate List integrity**

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

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

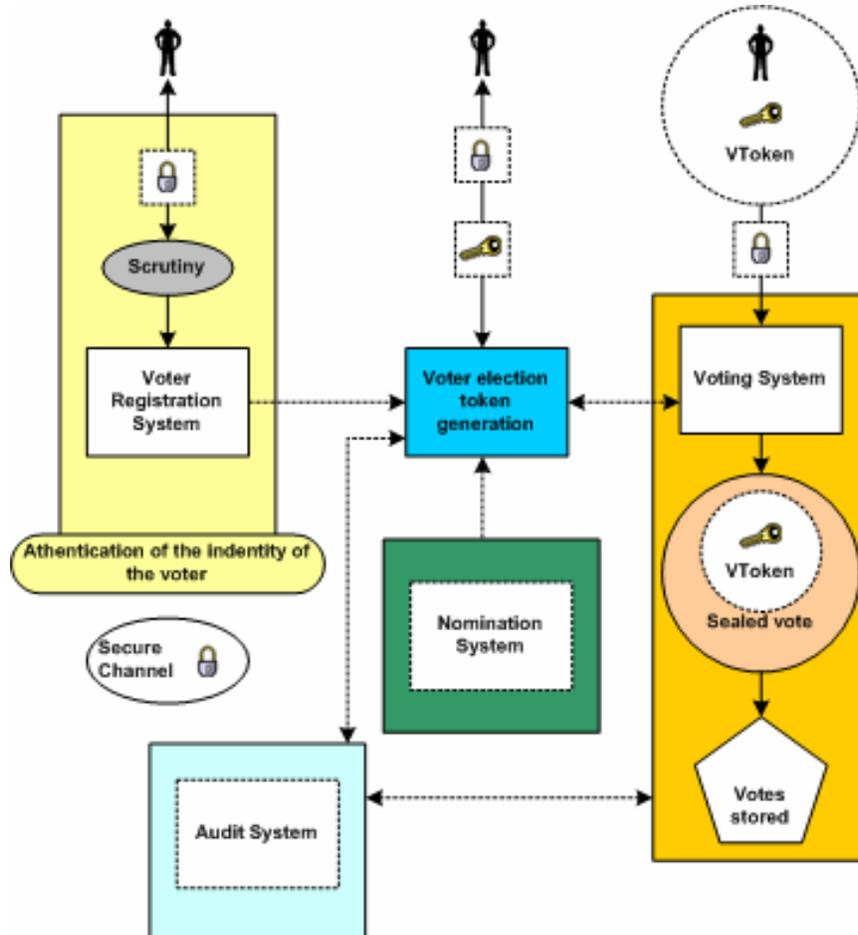
721 In summary, there must be a way of ensuring the validity of the ballot options and voter selection.

#### 722 **4.4.7 Vote counting accuracy**

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

727 **4.4.8 Voting System Security**

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



732  
 733 **Figure 3A: Voting system security**

734 **4.5 Remote voting security concerns**

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

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

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

758

## 5 Schema Outline

759

### 5.1 Structure

760 The Election Markup Language specification defines a vocabulary (the EML core) and message syntax  
761 (the individual message schemas). Thus most voting-related terms are defined as elements in the core  
762 with the message schemas referencing these definitions. The core also contains data type definitions so  
763 that types can be re-used with different names (for example, there is a common type to allow messages  
764 in different channel formats), or used as bases for deriving new definitions.

765 In some cases, two or more message schemas have large parts in common. For example, a voter  
766 authentication response message can contain a ballot that is almost identical to that used in the ballot  
767 message. When this occurs, the relevant declarations are included in a file whose file name includes the  
768 word 'include' and the number of the schemas in which it is used.

769 There is a third category of schema document within EML - the EML externals. This document contains  
770 definitions that are expected to be changed on a national basis. Currently this comprises the name and  
771 address elements, which are based on the OASIS Extensible Name and Address Language [1], but may  
772 be replaced by national standards such as those contained in the UK Government Address & Personal  
773 Details schemas [2]. Such changes can be made by replacing just this single file.

774 As well as these, several external schemas are used. The W3C has defined a standard XML signature  
775 [5]. OASIS has defined schemas for the extensible Name and Address Language (xNAL) [1]. As part of  
776 the definition of EML, the committee has defined a schema for the Timestamp used within EML. All these  
777 schemas use their appropriate namespaces, and are accessed using `xs:import` directives.

778 Each message (or message group) type is specified within a separate schema document. All messages  
779 use the EML element from the election core as their document element. Elements declared in the  
780 individual schema documents are used as descendents of the EML element.

781

### 5.2 IDs

782 XML elements may have an identifier which is represented as an `Id` attribute.

783 Each schema element has an `Id` attribute that relates to the message numbering scheme. Each message  
784 also carries this number.

785 Some items will have identifiers related to the voting process. For example, a voter might be associated  
786 with an electoral roll number or a reference on a company share register. These identifiers are coded as  
787 elements.

788 Other identifiers exist purely because of the various channels that can be used for voting (e.g. Internet,  
789 phone, postal, etc). In this case the identifiers are likely to be system generated and are coded as  
790 attributes.

791

### 5.3 Displaying Messages

792 Many e-voting messages are intended for some form of presentation to a user, be it through a browser, a  
793 mobile device, a telephone or another mechanism. These messages need to combine highly structured  
794 information (such as a list of the names of candidates in an election) with more loosely structured, often  
795 channel-dependent information (such as voting instructions).

796 Such messages start with one or more `Display` elements, such as:

797

```
<?xml version="1.0" encoding="UTF-8"?>
<EML
  Id="410"
  SchemaVersion="0.1"
  xml:lang="en"
  xmlns="http://www.govtalk.gov.uk/temp/voting"
```

798

799

800

801

802

803  
804  
805  
806  
807  
808  
809  
810  
811

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://www.govtalk.gov.uk/temp/voting  
    ..\schemas\ballot.xs">  
<Display Format="html">  
    <Stylesheet Type="text/xsl">../stylesheets/ballot.xsl</Stylesheet>  
    <Stylesheet Type="text/css">../stylesheets/eml.css</Stylesheet>  
</Display>  
<Ballots>  
    ...
```

812  
813  
814  
815  
816  
817

This example shows a Display element providing information to the receiving application about an XSL stylesheet which transforms the message into HTML for displaying the ballot in a Web browser. In the Display element in the example, the XSLT stylesheet reference is followed by a CSS stylesheet reference. In this case, the XSLT stylesheet referenced will pick up the reference to the CSS stylesheet as it transforms the message, and generate appropriate output to enable the displaying browser to apply that cascading stylesheet to the resulting HTML.

818  
819  
820  
821  
822

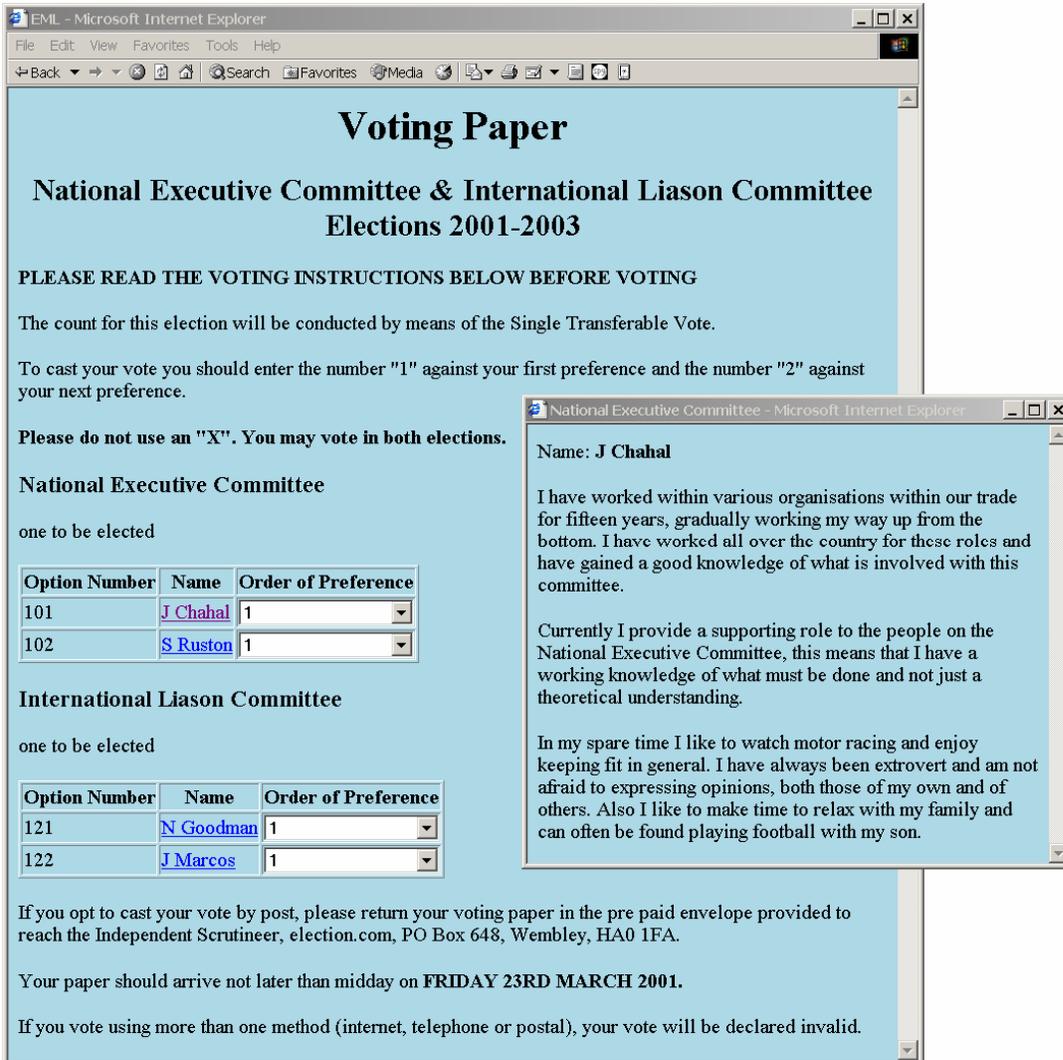
Not all information in a message will need to be displayed, and the creator of the message might have views on the order of display of the information. To allow stylesheets to remain generic, many elements in the schemas can have a DisplayOrder attribute. The values of these attributes determine the layout of the display (or the spoken voice if transforming to, for example, VoiceXML), even when using a generic stylesheet.

823  
824  
825  
826

When displaying messages in HTML, the expectation is that generic stylesheets will cover most cases, with the stylesheet output being embedded in a web page generated from an application-specific template. Similarly, voice applications might have specific welcome and sign-off messages, while using a generic stylesheet to provide the bulk of the variable data.

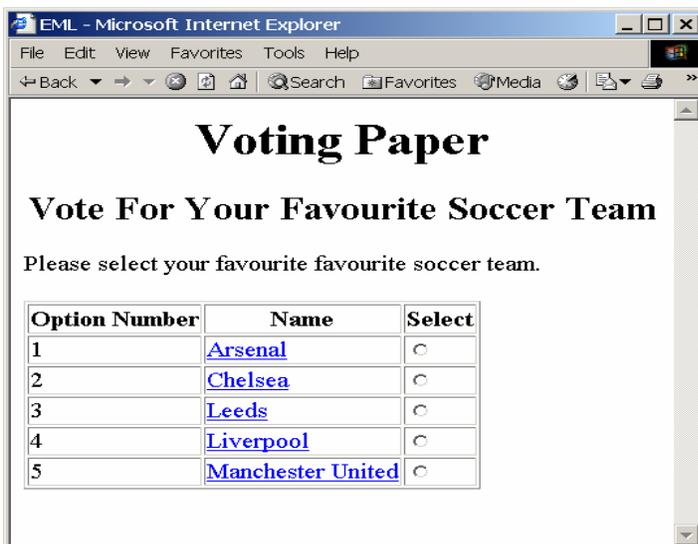
827  
828  
829

The three screen shots show the effect of using the same XSL stylesheet on the ballots for various voting scenarios. In the first picture, clicking on the name of a candidate has popped up a window with additional details.



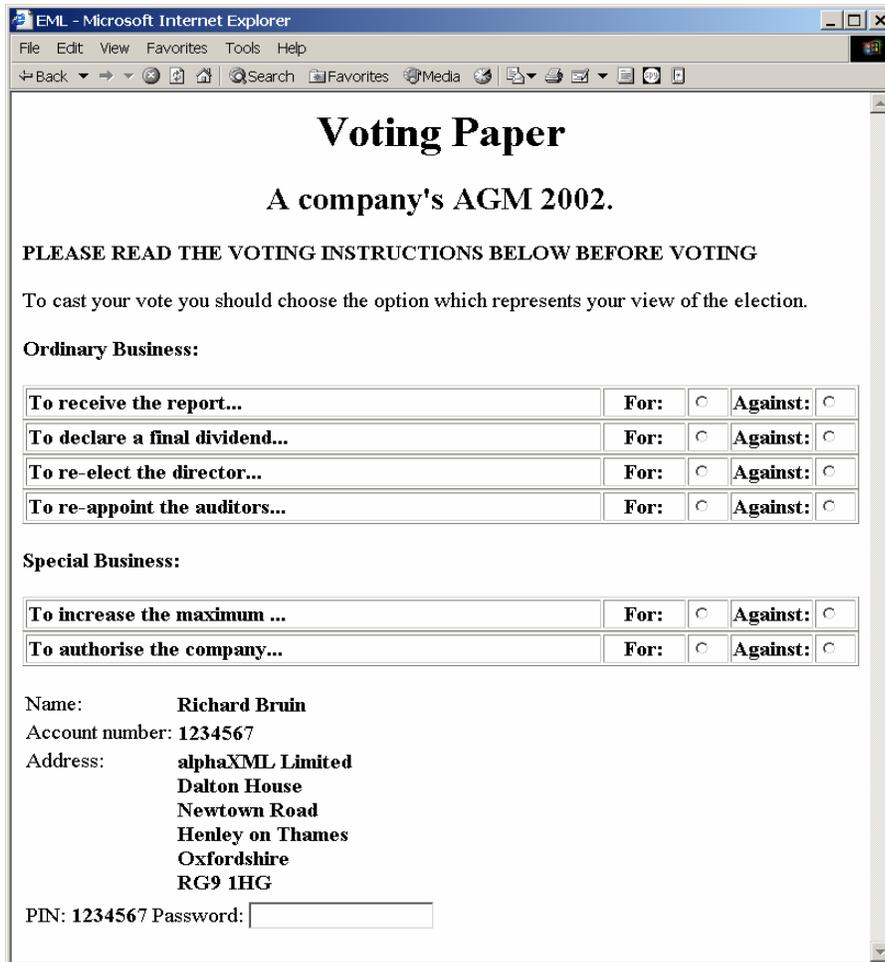
830

831 **Figure 3A: Screen shot of the ballot for scenario 1**



832

833 **Figure 3B: Screen shot of the ballot for scenario 2**



834

835 **Figure 3C: Screen shot of the ballot for scenario 3**

---

836 **6 Schema Descriptions**

837 Details on the description of schemas used in EML v5.0 can be found within the document 'EML v5.0  
838 Schema Descriptions'.

839

---

840 **A. Acknowledgements**

841 The following individuals have participated in the creation of this specification and are gratefully  
842 acknowledged:

843 **Participants:**

844  
845 Charbel Aoun, Accenture  
846 Siobhan Donaghy, OPT2VOTE Ltd  
847 Bruce Elton, Oracle Corporation  
848 Joseph Hall, University of California, Berkeley  
849 Roy Hill, OPT2VOTE Ltd  
850 John Ross, Associate  
851 Paul Spencer, Associate  
852 Johan Terryn, EDS  
853 Bernard Van Acke, IBM  
854 David Webber, Individual  
855 Peter Zelechowski, Associate

856 **B.**

857 **B.1 Internet Voting Security Concerns**

Concerns raised on Internet voting	Resulting Technical Threats	Possible generic security service countermeasure
<p>1. Impersonation of the right to vote.</p> <p>The concern here is that a person attempts to impersonate to be a legitimate voter when he/she is not.</p> <p>The initial task of verifying that a person has the right to vote must be part of the voter registration process.</p> <p>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.</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>Possible generic security service countermeasure</p> <p>Trusted voter identification and registration using:</p> <p>Security Procedures.</p> <p>Best Practices.</p> <p>Secure communications channels.</p> <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> <p>Connection Confidentiality</p> <p>Connection Integrity</p>
<p>2. Voter is not presented with correct ballot information due to incorrect candidate identification.</p>	<p>Incorrect identification during candidate registration.</p>	<p>Trusted candidate identification and registration are needed using:</p> <ul style="list-style-type: none"> <li>- Security Procedures.</li> <li>- Best Practices.</li> <li>- Secure communications channels.</li> <li>- Authentication and identification of candidates</li> </ul> <p>The candidate registration must follow standard Security Operating Procedures (SOPs) which</p>

			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: - Connection Confidentiality - Connection Integrity - Between voter and e-voting system
5	Obtaining the right to vote illegally from a legitimate voter.	Stealing the voter's voting card (e.g. the VToken data).	Some secret data only known to the voter's is required to be presented at the time of casting a vote.
	This may be by intimidation, theft or by any other means by which voting right has been obtained illegally.  For example, by  Stealing a voting card from a legitimate voter.	Any means of getting a legitimate voter to reveal his VToken data.	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.
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
7	Voter is not presented with correct ballot information	Inadequate integrity of the	Trusted path to voter on ballot options

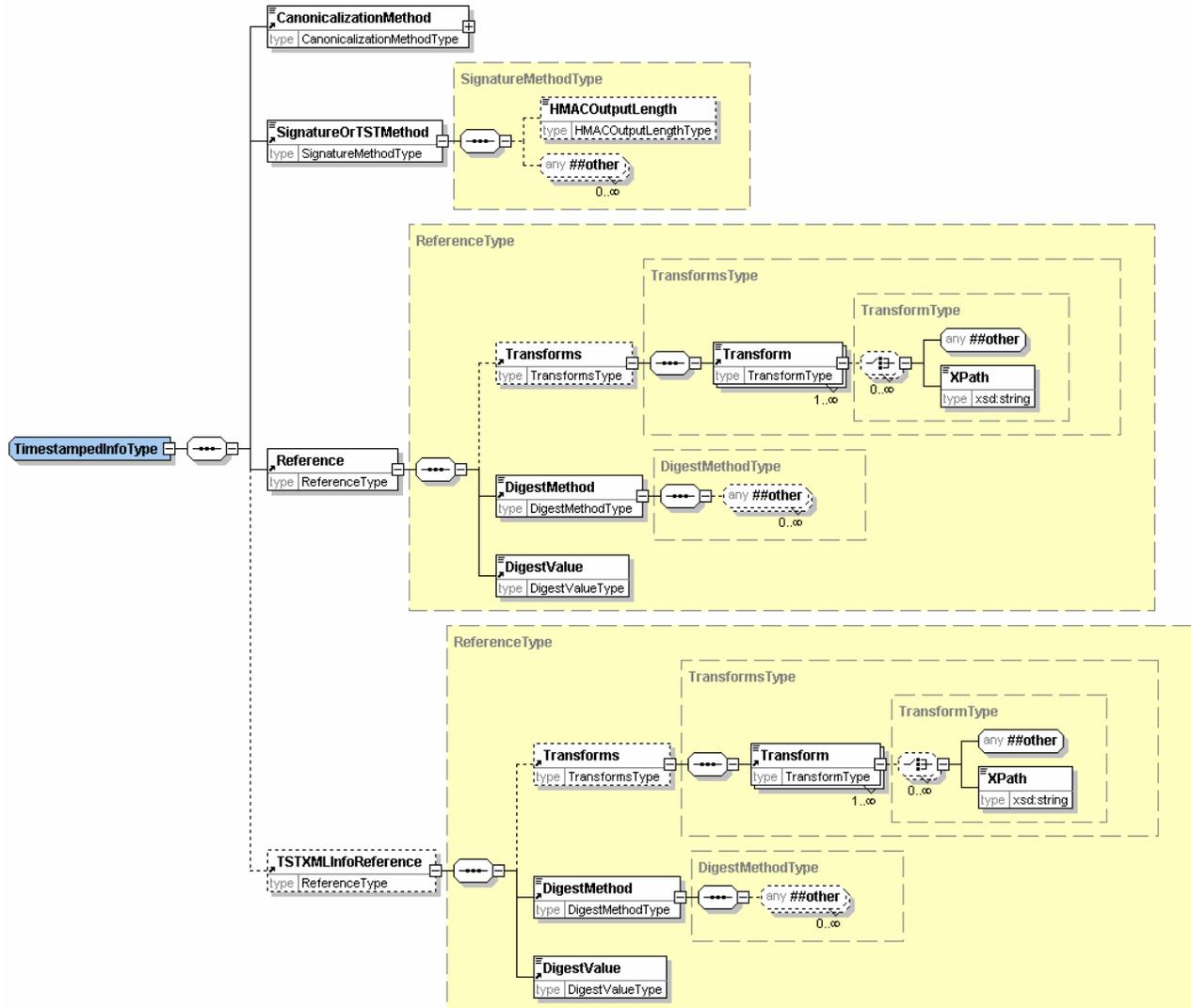
		ballot information	Integrity of the ballot information
		Given to the user	Integrity of cast votes
		Held in the voting system	
		The casting options available to the voter are not genuine	Trusted path between voter and vote recording
		Trojan horse, man in the middle attack	Trusted path to voter on ballot options
8	How do I know the voting system records votes properly	Integrity of the voting system	Non-repudiation of the vote
			Non-repudiation the vote was cast by a genuine voter
			Audit of voting system
			Connection confidentiality
		Insecure channel between the voter and the vote casting point	Connection Integrity
			Connection Confidentially
		Voter's intent is recorded accurately	Trusted path between voter and vote recording
			Non-repudiation of the vote recorded
		Proof that a genuine vote has been accurately counted	Audit
9	How can I be sure the voting system will not disclose whom I have voted for	Voter's identification is revealed	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;	Physical security
		Trojan horses	Procedural security
		Virus	Unpredictable Coded voting information
		Interception of communication	Integrity of communications channel between client and server system
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
		Multiple registration applications	Procedures Voter Identification
		Multiple allocation of voters credentials	Voter authentication
14	The vote cannot be altered from the voter's intention	Vulnerable client environment;	Trusted path from voter's intent to vote record
		Trojan horses	Vote integrity
		Virus	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: Connection Confidentiality
18	The voter's actual identity may need to be anonymous	Voter's identification is revealed	Voter's identification is anonymous
		Denial of service attack	
19	Denied access to electronic voting station		This needs to be counted by engineering the system to provide survivability when under denial of service attack.

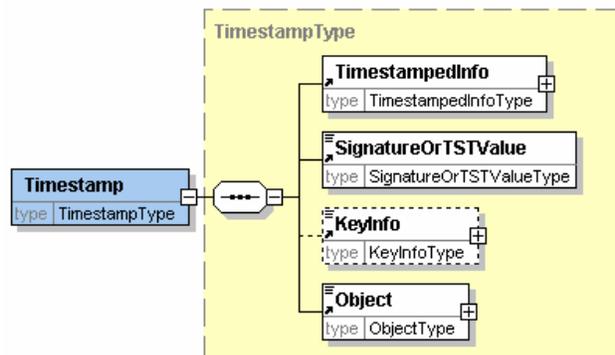
858

## 859 **B.2 The Timestamp Schema**

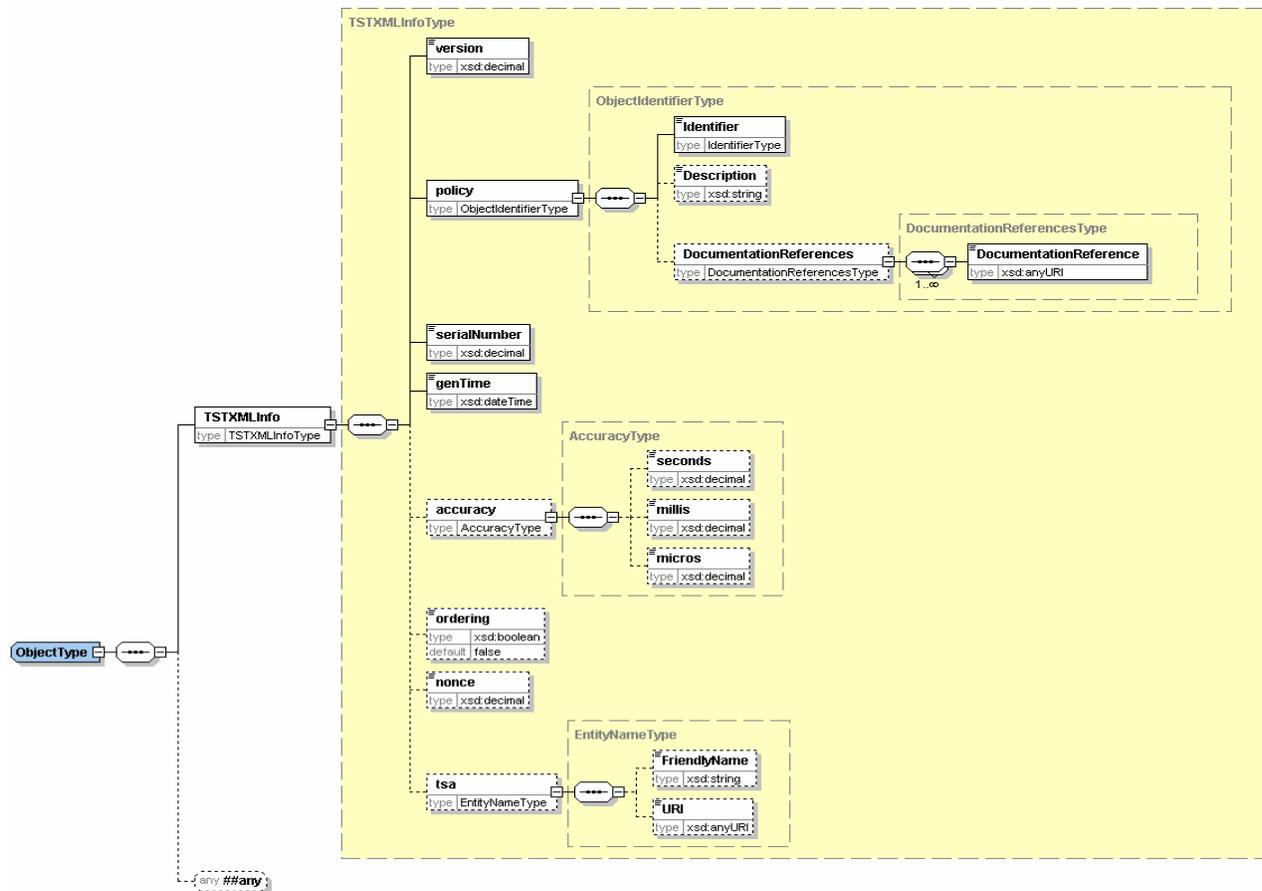
860 Although used as part of EML, this schema has been put in a separate namespace as it is not an integral  
861 part of the language. A time-stamp binds a date and time to the sealed data. The time-stamp seal also  
862 protects the integrity of the data. The structure of the time-stamp is similar to the structure of an XML  
863 Signature. The structure of the Timestamp element is shown here, followed by the detail of two of the four  
864 data types that are used to define its child elements.



865



866



- 867
- 868 The timestamp structure may be used in one of two ways either:
- 869
- 870 • Using Internet RFC 3161 binary encoded time-stamp token with the time-stamp information repeated in XML,
  - 871 • Using a pure XML encoded time-stamp.
- 872 In the case of the RFC 3161 based time-stamp, the Timestamp structure is used as follows:
- 873
- 874 • within TimestampedInfo:
  - 875 • TSTOrSignatureMethod identifies RFC 3161.
  - 876 • Reference contains the URI reference of the voting data being time-stamped. The DigestValue sub element contains the digest of the voting data being time-stamped.
  - 877 • TSTXMLInfoReference is not present in this case.
  - 878 • SignatureOrTSTValue holds the RFC 3161 time-stamp token applied to the digest of
  - 879 TimestampedInfo. The TimestampedInfo is transformed to a canonical form using the method
  - 880 identified in CanonicalizationMethod before the digest algorithm is applied.
  - 881 • KeyInfo contains any relevant certificate or key information.
- 882 Object contains the TSTXMLInfo element which is a copy of the information in SignatureOrTSTValue
- 883 converted from RFC 3161 to XML encoding. The TSTXMLInfo element contains:
- 884 • the version of time-stamp token format. This would be set to version 1
  - 885 • the time-stamping policy applied by the authority issuing the time-stamp,
  - 886 • the time-stamp token serial number,
  - 887 • the time that the token was issued, the contents of this element indicate the time of the timestamp.

- 888 • optionally an indication as to whether the time-stamps are always issued in the order that requests  
889 are received
- 890 • optionally a nonce<sup>1</sup> given in the request for the time-stamp token,
- 891 • optionally the identity of the time-stamping authority
- 892 In the case of a pure XML encoded time-stamp, the Timestamp structure is used as follows:
- 893 • within TimestampedInfo,
- 894 • TSTOrSignatureMethod identifies the algorithm used to create the signature value.
- 895 • Reference contains the URI reference of the voting data being time-stamped. The DigestValue sub  
896 element contains the digest of the voting data being time-stamped.
- 897 • TSTXMLInfoReference must be present, and contains the URI reference of TSTXMLInfo as  
898 contained within the Object element. The DigestValue sub element contains the digest of the  
899 TSTXMLInfo.
- 900 • SignatureOrTSTValue contains the signature value calculated over the TimestampedInfo using the  
901 signature algorithm identified in TSTOrSignatureMethod having been transformed to a canonical form  
902 using the method identified in CanonicalizationMethod. This signature is created by the time-stamping  
903 authority.
- 904 • KeyInfo contains any relevant certificate or key information.
- 905 Object contains the XML encoded time-stamp information in an TSTXMLInfo element. The contents of  
906 TSTXMLInfo is the similar as for the case described above. However, in this case the information is  
907 directly signed by the time-stamping authority. The TSTXMLInfo element contains:
- 908 • version of time-stamp token format: This would be set to version 2
- 909 • the time-stamping policy applied by the authority issuing the time-stamp,
- 910 • the time-stamp token serial number,
- 911 • the time that the token was issued, this is the time of the timestamp.
- 912 • optionally an indication as to whether the time-stamps are always issued in the order that requests  
913 were received
- 914 • optionally a nonce given in the request for the time-stamp token,
- 915 • optionally the identity of the time-stamping authority.

### 916 **B.3 W3C XML Digital Signature**

917 Some information on the digital signature is included here, but for full information refer to the  
918 Recommendation at [5].

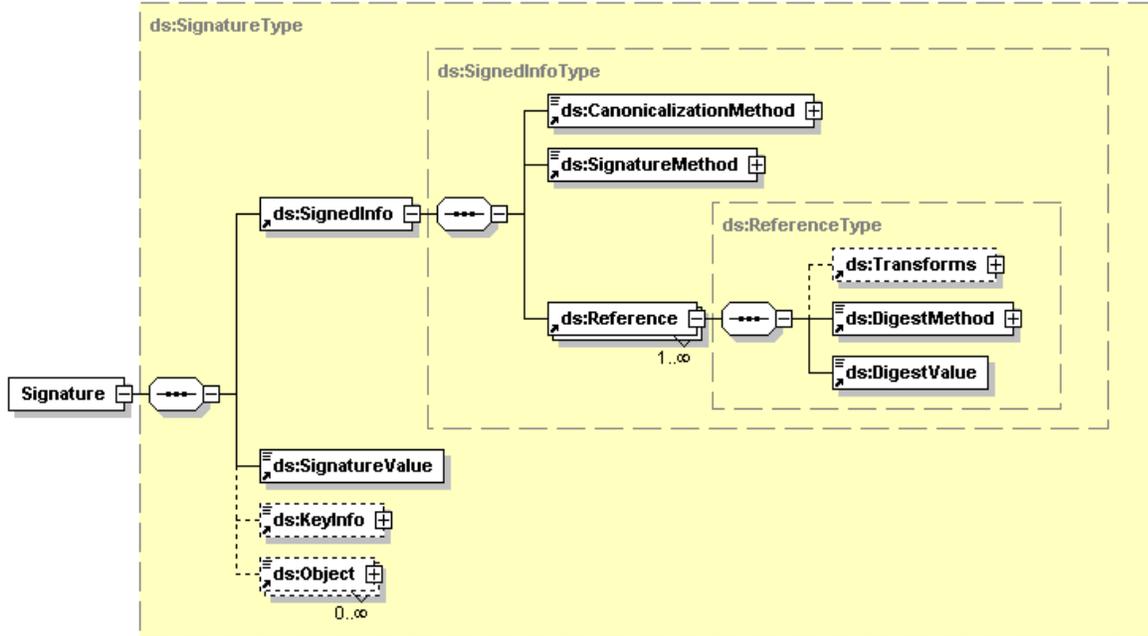
919 An XML Signature consists of:

- 920 • SignedInfo which includes a sequence of references to the data being signed with the digest (eg.  
921 SHA-1 hash) of the data being signed

---

<sup>1</sup> A nonce is a parameter that varies over time and is used as a defence against a replay attack.

- 922 • SignatureValue which contains the signature value calculated over the SignedInfo using the signature  
 923 algorithm identified in SignatureMethod having been transformed to a canonical form using the  
 924 method identified in CanonicalizationMethod
- 925 • KeyInfo contains any relevant certificate or key information.
- 926 • Object can contain any other information relevant to the signature



927  
 928  
 929

930

## C. Revision History

931

932

Revision	Date	Editor	Changes Made
V0.1a	2002-02-07	P Spencer	Draft e-voting schemas for internal comment
V0.2a	2002-02-13	P Spencer	Draft e-voting schemas for internal comment
V0.3a	2002-03-22	P Spencer	Draft e-voting schemas for public consultation comment
V0.4	2002-04-18	P Spencer	Draft Committee Specification version 2
V1.0	2002-04-29	P Spencer	Committee Specification for Technical Committee approval
V1.0	2002-05-13	P Spencer	Committee Specification
V2.0a	2002-06-13	F Ahmed	Revised draft accommodating committee's comments
V2.0b	2002-07-15	F Ahmed	Draft Committee Specification for Technical Committee approval
V2.0	2002-09-05	F Ahmed	Committee Specification
V3.0a	2002-12-12	F Ahmed	Draft Committee Specification
V3.0b	2003-02-06	F Ahmed	Draft Committee Specification for Technical Committee approval
V3.0	2003-02-24	F Ahmed	Committee Specification
V4.0a	2003-10-05	J Borrás	Revised draft accommodating requirements of Council of Europe Member States and UK pilots
V4.0b	2004-01-27	J Borrás	Draft Committee Specification
V4.0c	2004-03-09	J Borrás	Revised draft by placing Schema Description section in document of its own due to excessive size of v4.0b. Draft Committee Specification for Technical Committee approval.
V4.0d	2004-09-03	J Borrás	Draft Committee Specification for Technical Committee approval.
V4.0	2005-01-24	J Borrás	Committee Specification
V4.0	2006-02-01	J Borrás	OASIS Standard
V5.0	2007-03-14	J Borrás	Committee Draft

933