



EML Process & Data Requirements

Version 4.0

24 January 2005

Document identifier:

EML v4.0 Process and Data Requirements

Editor:

eGovernment Unit, Cabinet Office, UK

Contributors:

John Ross

Paul Spencer

John Borrás

Farah Ahmed

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 v4.0 Schema Descriptions' lists the schemas and schema descriptions to be used in conjunction with this specification.

Status:

This document is updated periodically on no particular schedule. Committee members should send comments on this specification to the election@lists.oasis-open.org list. Others should subscribe to and send comments to the election-services-comment@lists.oasis-open.org. To subscribe, send an email message to election-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

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 Election and Voter Services TC web page (<http://www.oasis-open.org/committees/election/>).

31 **Table of Contents**

32 1 Executive Summary 4

33 1.1 Overview of the Document..... 4

34 2 Introduction 6

35 2.1 Business Drivers 6

36 2.2 Technical Drivers..... 6

37 2.3 The E&VS Committee 6

38 2.4 Challenge and Scope 7

39 2.5 Documentation Set..... 8

40 2.6 Conformance..... 9

41 2.7 Terminology..... 9

42 3 High-Level Election Process 11

43 3.1 Figure 2A: High Level Model – Human View 12

44 3.2 Figure 2B: High-Level Model – Technical View 13

45 3.3 Outline 14

46 3.4 Process Descriptions 15

47 3.4.1 The Candidate Nomination Process..... 15

48 3.4.2 The Options Nomination Process 17

49 3.4.3 The Voter Registration..... 18

50 3.4.4 The Voting Process..... 19

51 3.4.5 The Vote Reporting Process..... 21

52 3.4.6 The Auditing System..... 22

53 3.5 Data Requirements 23

54 4 Security Considerations 24

55 4.1 Basic security requirements 24

56 4.1.1 Authentication 24

57 4.1.2 Privacy/Confidentiality 25

58 4.1.3 Integrity 25

59 4.1.4 Non-repudiation 26

60 4.2 Terms 26

61 4.3 Specific Security Requirements 27

62 4.4 Security Architecture 27

63 4.4.1 Voter identification and registration 28

64 4.4.2 Right to vote Authentication..... 28

65 4.4.3 Protecting exchanges with remote voters..... 29

66 4.4.4 Validating Right to Vote and contest vote sealing 29

67 4.4.5 Vote confidentiality..... 30

68 4.4.6 Candidate list integrity 30

69 4.4.7 Vote counting accuracy 30

70 4.4.8 Voting System Security..... 31

71 4.5 Remote voting security concerns..... 31

72 5 Schema Outline 33

73	5.1 Structure.....	33
74	5.2 IDs	33
75	5.3 Displaying Messages	33
76	6 Schema Descriptions	37
77	Appendix A: Internet Voting Security Concerns	38
78	Appendix B: The Timestamp Schema	42
79	Appendix C: W3C XML Digital Signature	45
80	Appendix D: Revision History	46
81	References	47
82	Notices.....	48

83

1 Executive Summary

84

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:

87

“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...”

90

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:

93

- **Multinational:** Our aim is to have these standards adopted globally.

94

- **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).

95

96

- **Multilingual:** Flexible enough to accommodate the various languages and dialects and vocabularies.

97

98

- **Adaptable:** Resilient enough to support elections in both the private and public sectors.

99

- **Secure:** Able to secure the relevant data and interfaces from any attempt at corruption, as appropriate to the different requirements of varying election rules.

100

101

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:

102

103

104

- 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.

105

106

107

108

109

110

111

112

113

114

115

116

117

1.1 Overview of the Document

118

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.

119

120

121

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.

122

123

124

125 **Section 3** describes two complementary high-level process models of an election exercise,
126 based on the human and technical views of the processes involved. It is intended to identify all
127 the generic steps involved in the process and highlight all the areas where data is to be
128 exchanged. The discussions in this section present details of how the messages and data
129 formats detailed in the EML specifications themselves can be used to achieve the goals of open
130 interoperability between system components.

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

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

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

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

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

149 2 Introduction

150 2.1 Business Drivers

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

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

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

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

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

172 2.2 Technical Drivers

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

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

183 2.3 The E&VS Committee

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

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

192

193 The Committee's mission statement is:

194 *"Develop a standard for the structured interchange of data among hardware, software, and*
195 *service providers who engage in any aspect of providing election or voter services to public or*
196 *private organizations. The services performed for such elections include but are not limited to*
197 *voter role/membership maintenance (new voter registration, membership and dues collection,*
198 *change of address tracking, etc.), citizen/membership credentialing, redistricting, requests for*
199 *absentee/expatriate ballots, election calendaring, logistics management (polling place*
200 *management), election notification, ballot delivery and tabulation, election results reporting and*
201 *demographics."*

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

207 Dr. Michael Ian Shamos, a PhD Researcher who worked on 50 different voting systems since
208 1980 and reviewed the election statutes in half the US states, summarized a list of fundamental
209 requirements, or 'six commandments', for electronic voting systems:

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

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

- 219 • Multinational – our aim is to have these standards adopted globally
- 220 • Effective across the different voting regimes – for example, proportional representation or
221 'first past the post', preferential voting, additional member system
- 222 • Multilingual – our standards will need to be flexible enough to accommodate the various
223 languages and dialects and vocabularies
- 224 • Adaptable – our aim is to provide a specification that is resilient enough to support
225 elections in both the private and public sectors
- 226 • Secure – the standards must provide security that protects election data and detects any
227 attempt to corrupt it.

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

230 **2.4 Challenge and Scope**

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

237 These processes are illustrative, covering the vast majority of election types and forming a basis
238 for defining the Election Markup Language itself. EML has been designed such that elections that

239 do not follow this process model should still be able to use EML as a basis for the exchange of
 240 election-related messages.

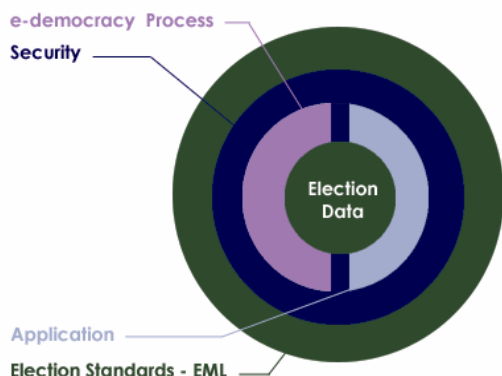
241 EML is focussed on defining open, secure, standardised and interoperable interfaces between
 242 components of election systems. Thus providing transparent and secure interfaces between
 243 various parts of an election system. The scope of election security, integrity and audit included in
 244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

247 The security requirement for the election system design, implementation or evaluation must be
 248 placed within the context of the vulnerabilities and threats analysis of a particular election
 249 scenario. As such the references to security within EML are not to be taken as comprehensive
 250 requirements for all election systems in all election scenarios, nor as recommendations of
 251 sufficiency of approach when addressing all the security aspects of election system design,
 252 implementation or evaluation. In fact, the data security mechanisms described in this document
 253 are all optional, enabling compliance with EML without regard for system security at all.

254 A complementary document may be defined for a specific election scenario, which refines the
 255 security issues defined in this document.

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

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



266
 267 **Figure 1A: Relationship overview**

268 **2.5 Documentation Set**

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

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

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

- 279 • **Voting Processes:** A general and global study of the electoral process. This introduces
 280 the transition from a complete human process by defining the data structure to be
 281 exchanged and where they are needed.
- 282 • **Data Requirements:** A data dictionary defining the data used in the processes and
 283 required to be handled by the XML schemas.
- 284 • **EML Specifications:** This consists of a library of XML schemas used in EML. The XML
 285 schemas define the formal structures of the election data that needs to be exchanged.
- 286 • **Report on Alternative methods of EML Localisation:** EML provides a set of
 287 constraints common to most types of elections worldwide. Each specific election type will
 288 require additional constraints, for example, to enforce the use of a seal or to ensure that a
 289 cast vote is anonymous. This document describes alternative mechanisms for expressing
 290 these constraints and recommends the use of schemas using the Schematron language
 291 to supplement the EML schemas for this purpose.

292 2.6 Conformance

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

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

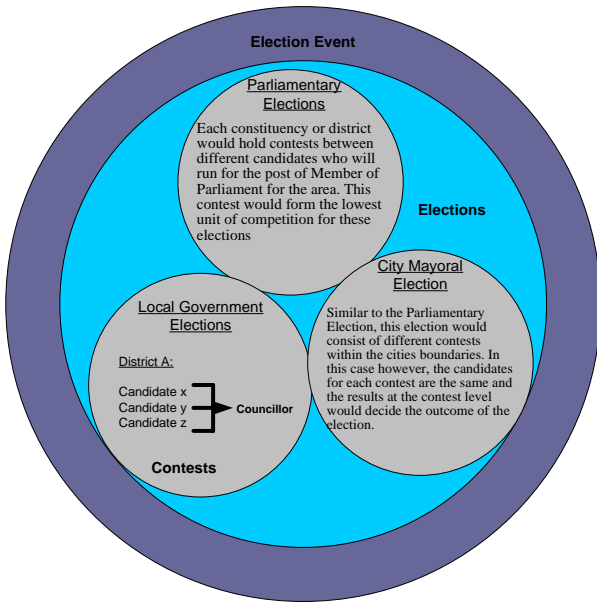
300 2.7 Terminology

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

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

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

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

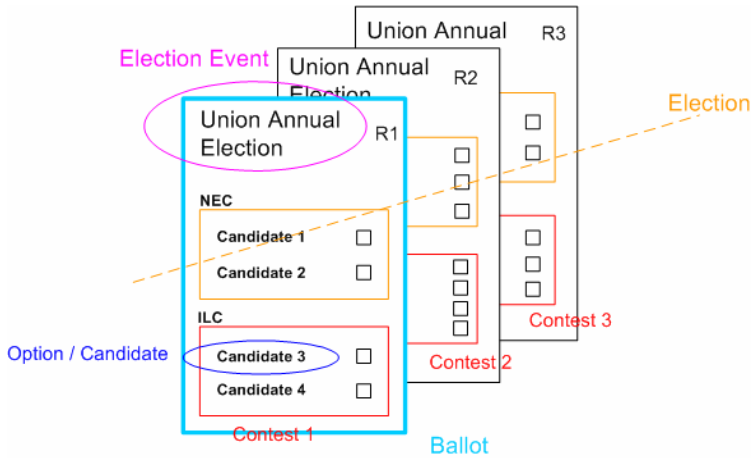


312

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

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

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



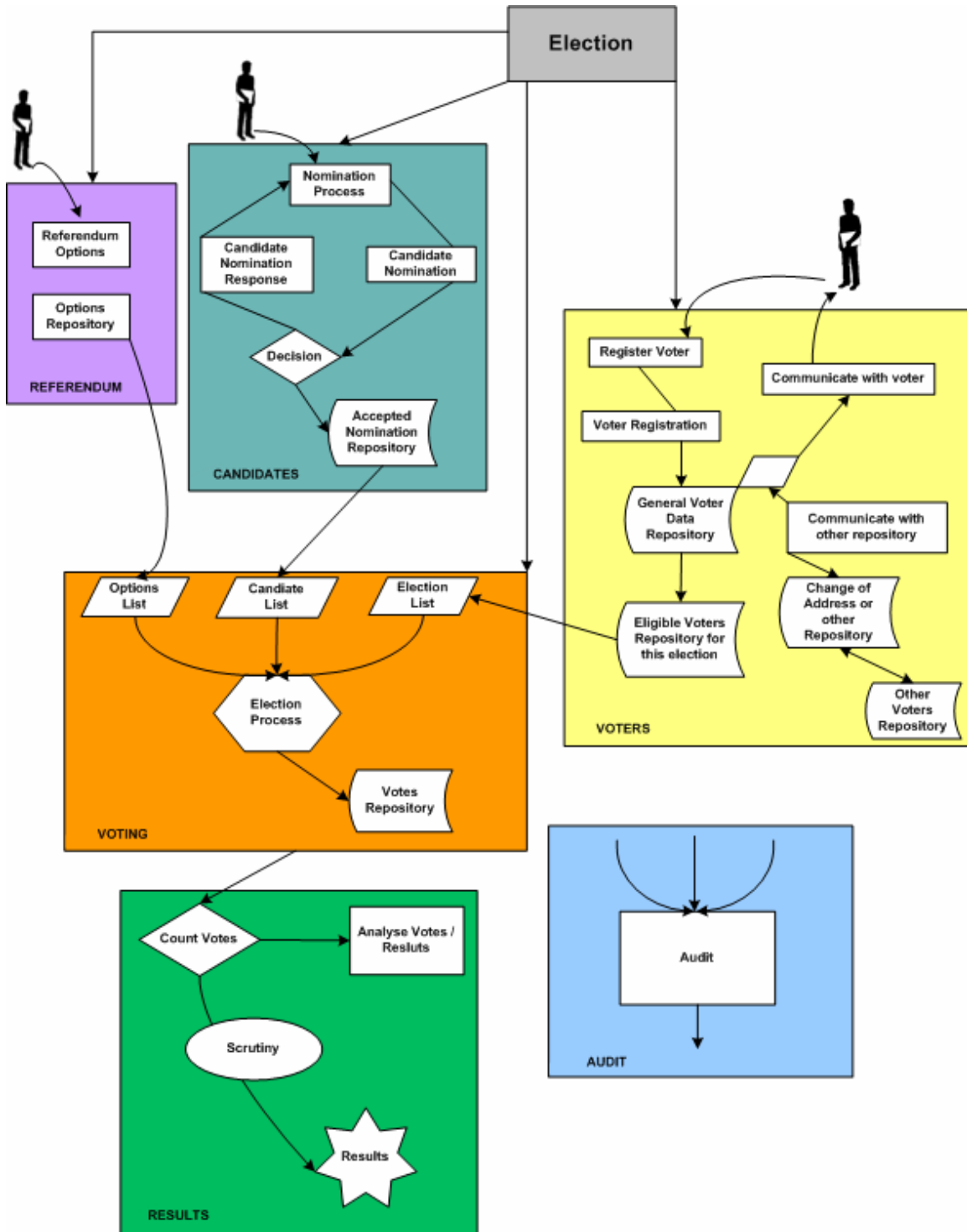
323

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

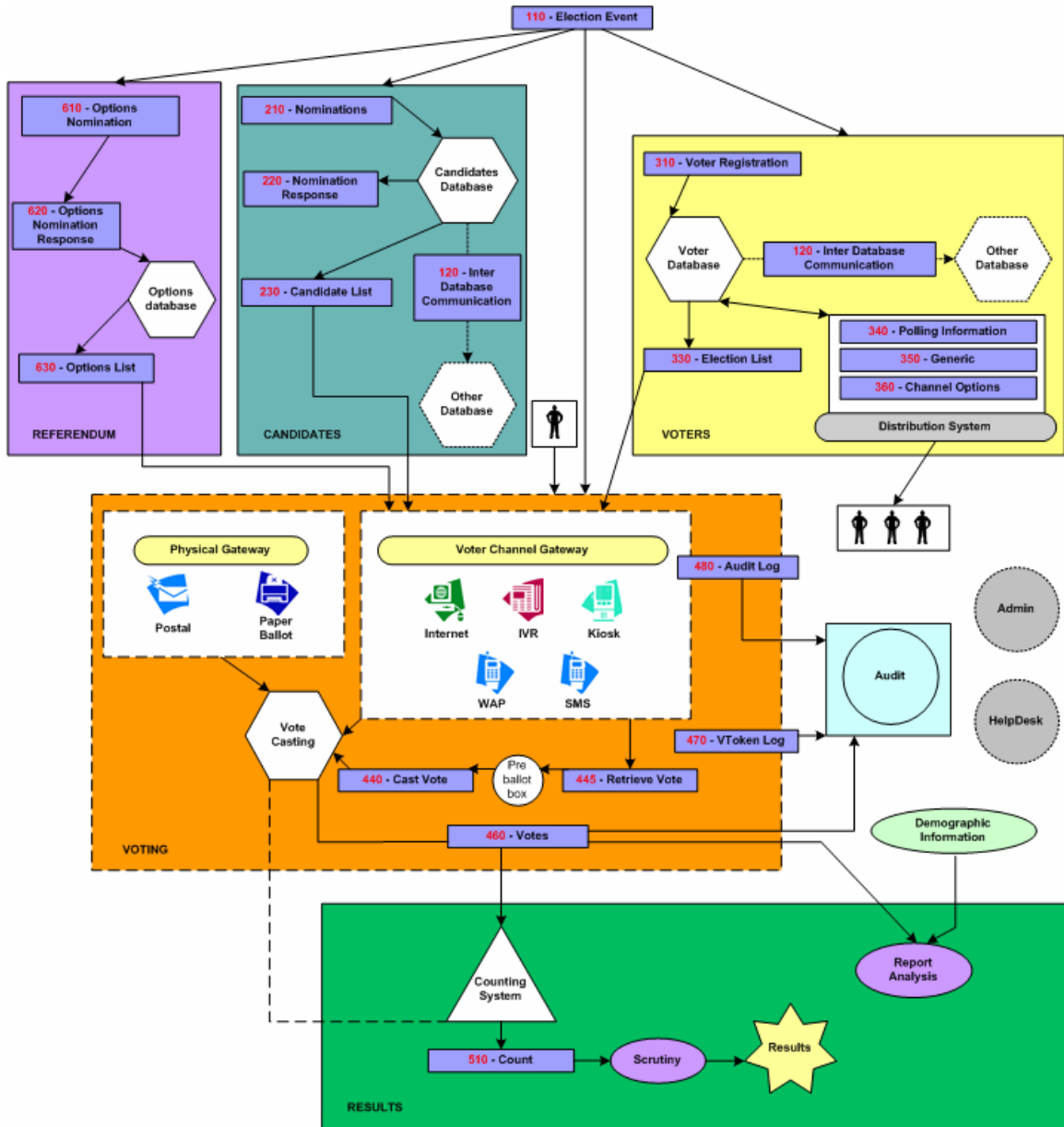
325 **3 High-Level Election Process**

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

3.1 Figure 2A: High Level Model – Human View



3.2 Figure 2B: High-Level Model – Technical View



334 **3.3 Outline**

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

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

- 341 • Pre election
 - 342 – Election (100)
 - 343 – Candidates (200)
 - 344 – Options (600)
 - 345 – Voters (300)
- 346 • Election
 - 347 – Voting (400)
- 348 • Post election
 - 349 – Results (500)
 - 350 – Audit
 - 351 – Analysis

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

- 353 • Administration Interface
- 354 • Help Desk

355

3.4 Process Descriptions

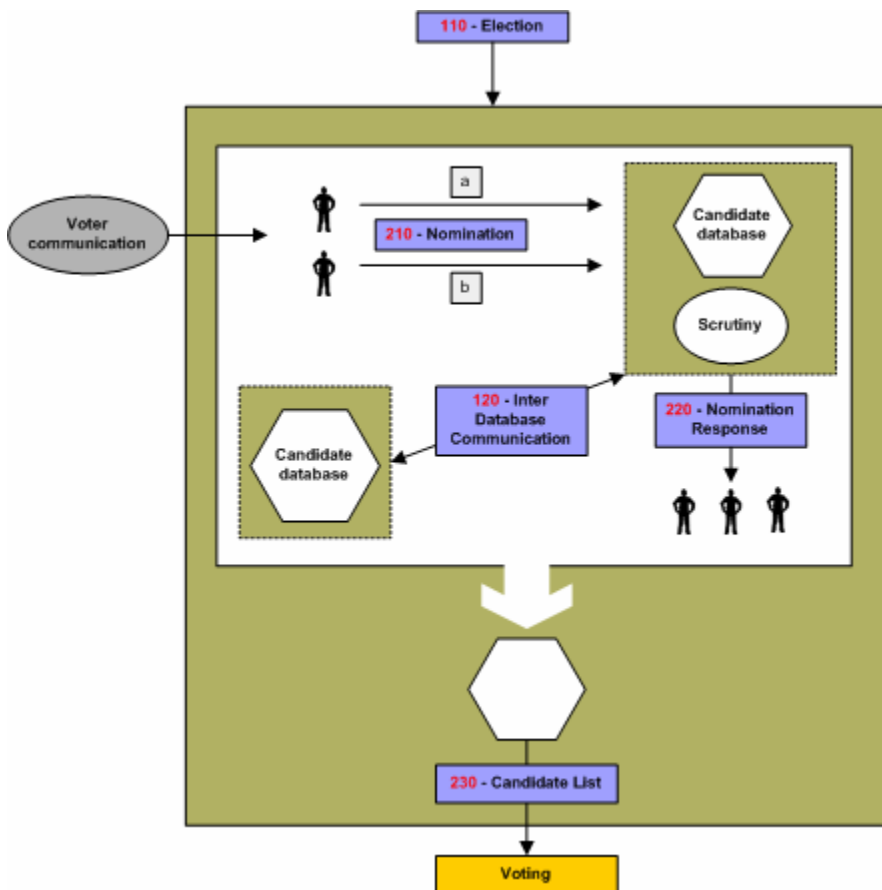
356

3.4.1 The Candidate Nomination Process

357

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

358



359

360

Figure 2C: The Candidate Nomination Process

361

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

362

363

364

- 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.

365

366

- Interested parties will respond in the proper way satisfying the rules of nomination for this election with the objective of becoming running candidates. The response message conforms to schema 210.

367

368

369

- A nomination for an individual candidate can be achieved in one of two ways:

370

371

- A Nominee will reply by attaching to his nomination a list of x number of endorsers with their signature.
- Each endorser will send a message specifying Mr. X as his or her nominee for the position in question. Mr X will signal his agreement to stand.

372

373

374

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

375

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

- 379 • Pay fees,
- 380 • Have x number of endorsers,
- 381 • Be of a certain age,
- 382 • Be a citizen more than x number of years,
- 383 • Not stand for election in more than one contest at a time,
- 384 • Etc.

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

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

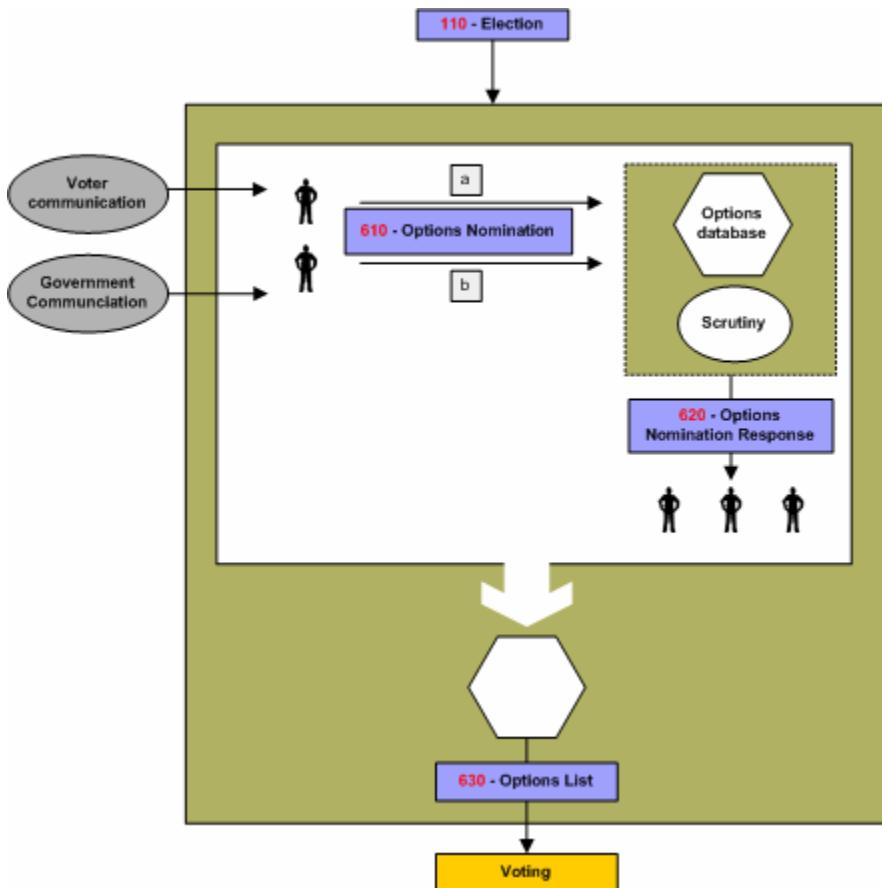
389 Nominees will be notified of the result of the scrutiny using a message conforming to schema
390 220.

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

394

3.4.2 The Options Nomination Process

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



398

399 **Figure 2D: Referendum Options Nomination Process**

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

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

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

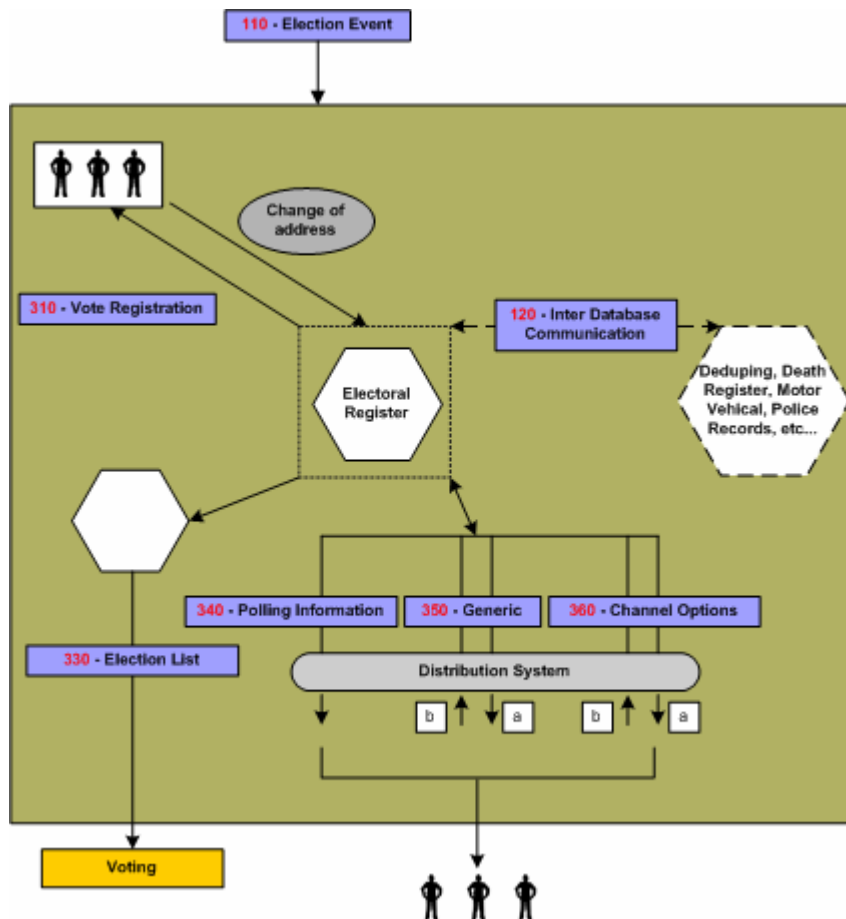
407

3.4.3 The Voter Registration

408

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

409



410

411

Figure 2E: Voter Registration

412

The centre of this process is the Electoral Roll Database or the Voters' Database. The input into this database is the outcome of communications between 'a voter' and 'an Election Authority'.

413

The subject of this correspondence can vary from adding a voter to modifying a voter; deletion of a voter is considered as part of modification.

414

415

416

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

417

418

419

420

Another potential communication or exchange of data is with other databases such as those used

421

by another election authority, government body, etc. Database exchanges will be required in

422

some election scenarios; examples include geographical and organizational boundary changes.

423

At a certain date, a subset of the voters' database is fixed from which the election list is generated. Schema s contains some subset of the eligible voters, perhaps grouped by polling

424

district or voting channel.

425

426

It is here that we introduce the concept of voter communications. Under this category we divided

427

them into three possible types of communications:

428

- Channel options

429

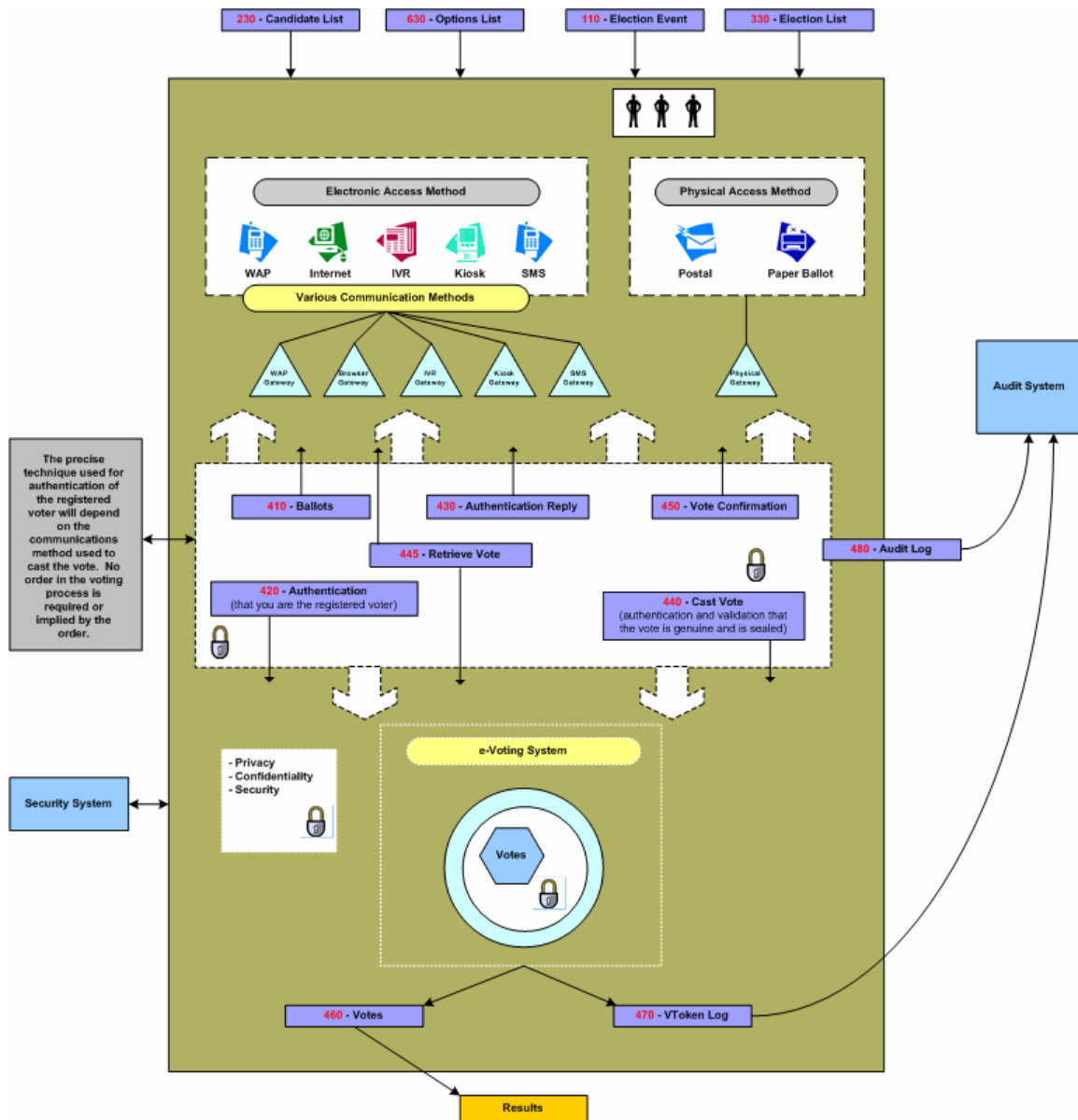
- Polling Information

430 • Generic.

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

434 3.4.4 The Voting Process

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



437
438 **Figure 2F: The Voting Process**

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

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

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

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

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

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

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

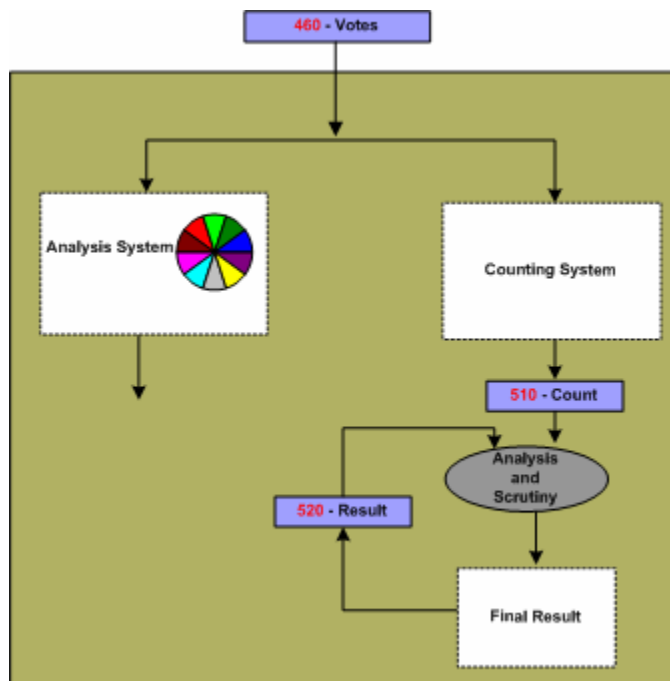
461

3.4.5 The Vote Reporting Process

462

Two of the post election items are the Final Result and the Audit Report. Audit is discussed in

463



464

465 **Figure 2G: The Vote Reporting Process**

466

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

467

468

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

469

470

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

471

472

473

474

475

476

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

477

478

479

480

Further schemas may be developed that make use of the Votes and Count schemas. For

481

example schemas for messages that report election results to the media.

482

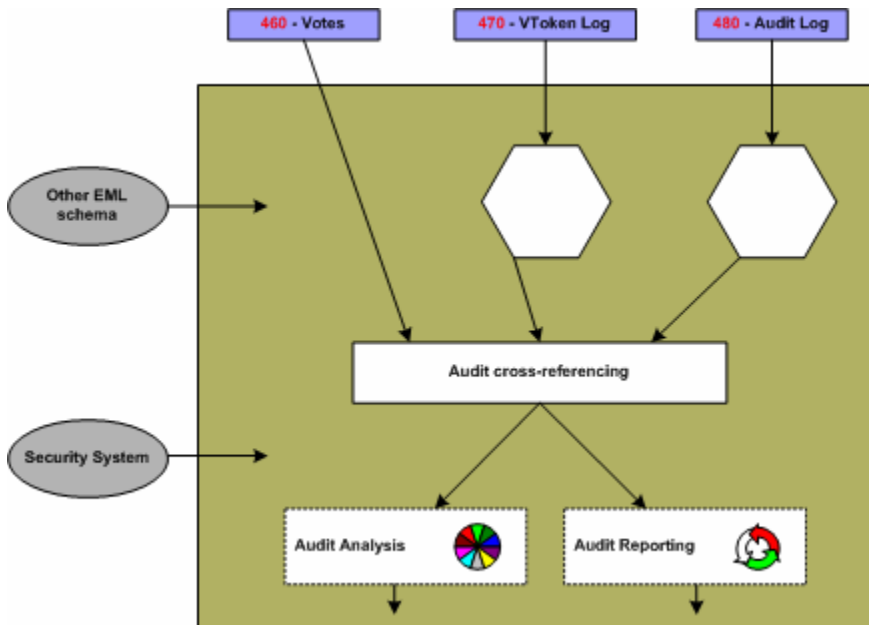
3.4.6 The Auditing System

483

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

484

485



486

487

Figure 2H: Auditing System

488

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

489

490

Schemas 460, 470, 480 from the voting process provide input data to the audit process.

491

Depending on the audit requirements additional data from other processes may be required. In particular, the security process may provide additional data about all the issued VTokens and Qualified VTokens (see Figure 3A: Voting system security).

492

493

494

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

495

496

497

- Eligible voters

498

- Issued VTokens or Qualified VTokens.

499

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

500

501

502

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

503

504

505

506

507

508

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

509

510

511

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

516 A further requirement is for the election officer to be provided with a mechanism to allow a
517 recount when a result is contested. The number of votes from the voting system using schema
518 460 can be verified by correlating the total votes as calculated by the audit system (using schema
519 480), with the totals from the counting system. Then either re-running the count or running the
520 count on another implementation can verify an individual result.

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

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

533 **3.5 Data Requirements**

534 The data used in all the above processes are defined in 'EML v4.0 Data Dictionary'.

535 4 Security Considerations

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

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

545 4.1 Basic security requirements

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

- 550 • Security considerations of e-voting systems include:
- 551 • Authentication
- 552 • Privacy/Confidentiality
- 553 • Integrity
- 554 • Non-repudiation

555 4.1.1 Authentication

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

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

- 559 • Checking a claim of identity
- 560 • Checking a right to vote.

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

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

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

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

576 Where an election scenario demands anonymity of the voter and privacy of the voter’s ballot, the
577 identity of the voter and the cast votes must be separated at some time within the voting process.

578 This can be done in several ways by a voting system including, but not restricted to, the following
579 options:

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

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

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

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

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

596 **4.1.2 Privacy/Confidentiality**

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

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

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

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

612 **4.1.3 Integrity**

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

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

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

625

4.1.4 Non-repudiation

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

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

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

653

4.2 Terms

654 The following security terms are used in this document:

- 655 • Identity Authentication: the means by which a voter registration system checks the
656 validity of the claimed identity.
- 657 • Right to vote authentication: the means by which the voting system checks the validity of
658 a voter’s right to vote.
- 659 • VToken: the means by which a voter proves to an e-voting system that he/she has the
660 right to vote in a contest.
- 661 • VToken Qualified: the means by which a VToken can be qualified. The reason for the
662 qualification is always appended to a VToken that is qualified. For example, a qualified
663 VToken may be issued to a challenged voter.
- 664 • Vote sealing: the means by which the integrity of voting data (ballot choices, vote cast
665 against a given VToken) can be protected (e.g. using a digital signature or other
666 authentication code) so that it can be proved that a voter’s authentication and one or
667 more votes are related.

668

4.3 Specific Security Requirements

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

- 670 • Only legitimate voters are allowed to vote (i.e. voters must be authenticated as having the
671 right to cast a vote)
- 672 • Only one set of choices is allowed per voter, per contest
- 673 • The vote cannot be altered from the voter's intention
- 674 • The vote may not be observed until the proper time
- 675 • The voting system must be accountable and auditable
- 676 • Information used to authenticate the voter or his/her right to vote should be protected
677 against misuse (e.g. passwords should be protected from copying)
- 678 • Voter privacy must be maintained according to the laws of the election jurisdiction. (Legal
679 requirements of public elections in various countries conflict. Some countries require that
680 the vote cannot be tracked back to the voter's identity, while others mandate that it must
681 be possible to track every vote to a legitimate voter's identity)
- 682 • The casting options available to the voter must be genuine
- 683 • Proof that all genuine votes have been accurately counted.

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

- 686 • Several technologies may be employed in the voting environment
- 687 • The voting environment may be made up of systems from multiple vendors
- 688 • A voter may have the option to vote through alternative delivery channels (i.e. physically
689 presenting themselves at a polling station, by post, by electronic means)
- 690 • The voting systems need to be able to meet various national legal requirements and local
691 voting rules for both private and public elections
- 692 • Need to verify that all votes are recorded properly without having access to the original
693 input
- 694 • The mechanism used for voter authentication may vary depending on legal requirements
695 of the contest, the voter registration and the e-voting systems for private and public
696 elections
- 697 • The user may be voting from an insecure environment (e.g. a PC with no anti-virus
698 checking or user access controls).

699 Objectives of this security architecture include:

- 700 • Be open
- 701 • Not to restrict the authentication mechanisms provided by e-voting systems
- 702 • Specify the security characteristic required of an implementation, allowing for freedom in
703 its precise implementation.

704 4.4 Security Architecture

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

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

- 708 • Voter identification and registration
- 709 • Right to vote authentication

- 710 • Protecting exchanges with remote voters
- 711 • Validating Right to Vote and contest vote sealing
- 712 • Vote confidentiality.
- 713 • Candidate list Integrity
- 714 • Vote counting accuracy
- 715 • Voting system security controls.

716 **4.4.1 Voter identification and registration**

717 The Voter identification and registration is used to identify an entity (e.g. person) for the purpose
718 of registering the person has a right to vote in one or more contests, thus identifying legitimate
719 voters. The security characteristics for voter identification are to be able to authenticate the
720 identity of the legal person allowed to vote in a contest and to authenticate each person's voting
721 rights. The precise method of voter identification is not defined here, as it will be specific to
722 particular voting environments, and designed to meet specific legal requirements, private or
723 public election and contest rules. The voter registration system may interact with the e-voting
724 system and other systems to define how to authenticate a voter for a particular contest.

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

733 **4.4.2 Right to vote Authentication**

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

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

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

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

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

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

767 **4.4.3 Protecting exchanges with remote voters**

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

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

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

780 **4.4.4 Validating Right to Vote and contest vote sealing**

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

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

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

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

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

803

4.4.5 Vote confidentiality

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

808

4.4.6 Candidate list integrity

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

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

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

819

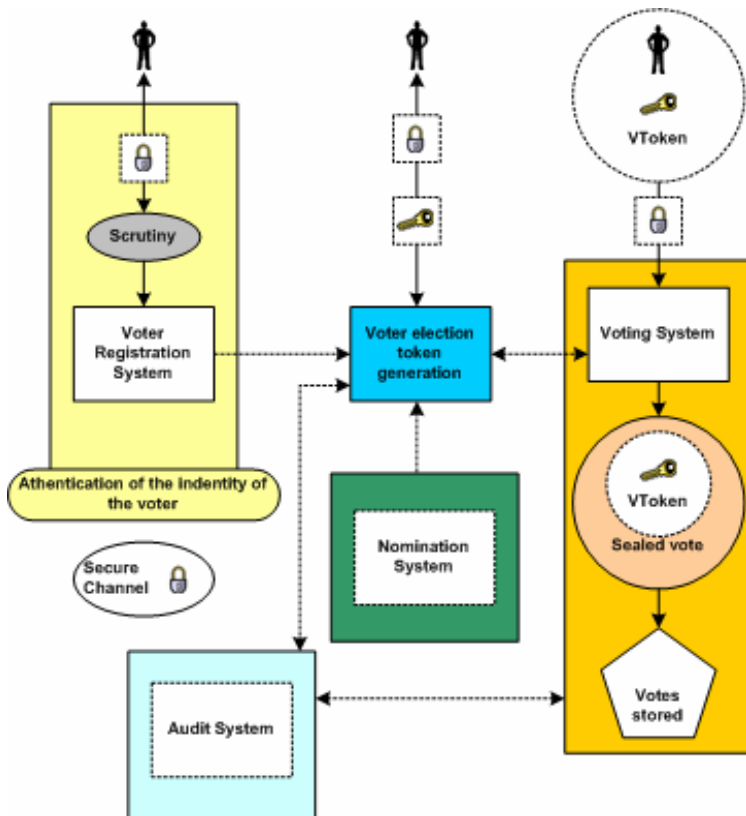
4.4.7 Vote counting accuracy

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

824

4.4.8 Voting System Security

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



829

830 **Figure 3A: Voting system security**

831

4.5 Remote voting security concerns

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

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

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

857 5 Schema Outline

858 5.1 Structure

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

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

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

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

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

883 5.2 IDs

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

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

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

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

893 5.3 Displaying Messages

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

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

899

```
<?xml version="1.0" encoding="UTF-8"?>
```

900
901
902
903
904
905
906
907
908
909
910
911
912
913

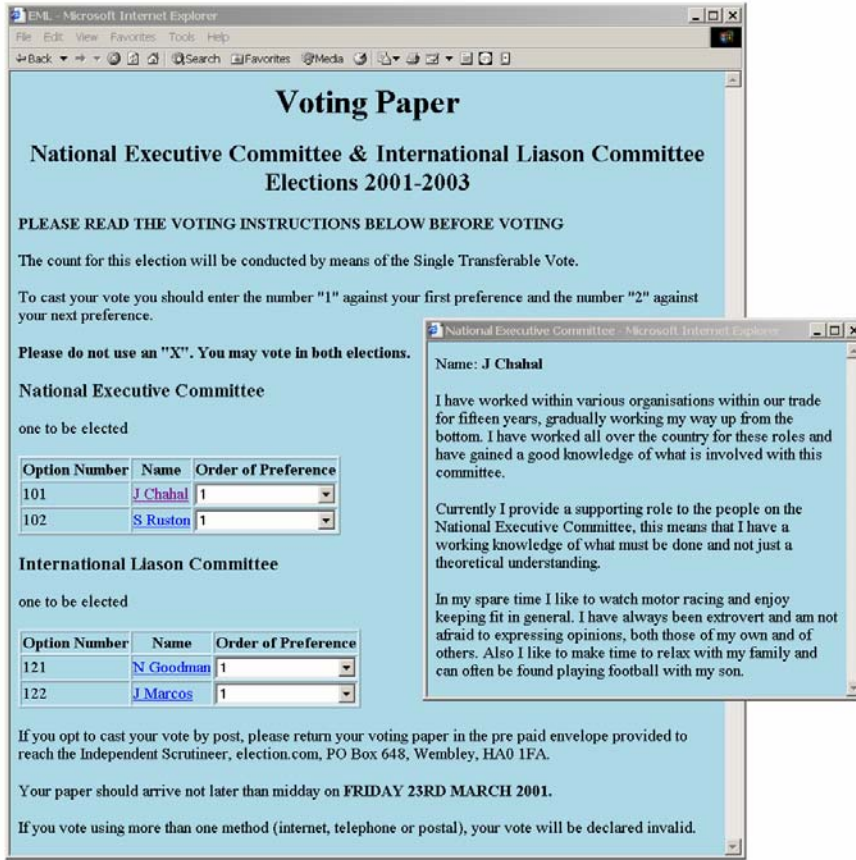
```
<EML
  Id="410"
  SchemaVersion="0.1"
  xml:lang="en"
  xmlns="http://www.govtalk.gov.uk/temp/voting"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.govtalk.gov.uk/temp/voting
    ..\schemas\ballot.xs">
  <Display Format="html">
    <Stylesheet Type="text/xsl">../stylesheets/ballot.xsl</Stylesheet>
    <Stylesheet Type="text/css">../stylesheets/eml.css</Stylesheet>
  </Display>
  <Ballots>
    ...
```

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

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

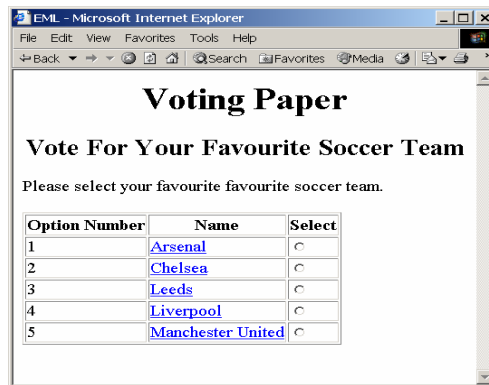
925 When displaying messages in HTML, the expectation is that generic stylesheets will cover most
926 cases, with the stylesheet output being embedded in a web page generated from an application-
927 specific template. Similarly, voice applications might have specific welcome and sign-off
928 messages,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

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



932

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



934

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

EML - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Voting Paper

A company's AGM 2002.

PLEASE READ THE VOTING INSTRUCTIONS BELOW BEFORE VOTING

To cast your vote you should choose the option which represents your view of the election.

Ordinary Business:

To receive the report...	For:	<input type="radio"/>	Against:	<input type="radio"/>
To declare a final dividend...	For:	<input type="radio"/>	Against:	<input type="radio"/>
To re-elect the director...	For:	<input type="radio"/>	Against:	<input type="radio"/>
To re-appoint the auditors...	For:	<input type="radio"/>	Against:	<input type="radio"/>

Special Business:

To increase the maximum ...	For:	<input type="radio"/>	Against:	<input type="radio"/>
To authorise the company...	For:	<input type="radio"/>	Against:	<input type="radio"/>

Name: Richard Bruin
 Account number: 1234567
 Address: alphaXML Limited
 Dalton House
 Newtown Road
 Henley on Thames
 Oxfordshire
 RG9 1HG

PIN: 1234567 Password:

936

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

938

6 Schema Descriptions

939
940

Details on the description of schemas used in EML v4.0 can be found within the document 'EML v4.0 Schema Descriptions'.

Appendix A: Internet Voting Security Concerns

Concerns raised on Internet voting		Resulting Technical Threats	Possible generic security service countermeasure
1.	<p>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>	Inadequate, incorrect or improper identification of person during registration of voters	<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>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>	Inadequate privacy of the exchange between the person and the electoral system during voter registration	<p>Channel between voter and registration system must provide:</p> <p>Connection Confidentiality</p> <p>Connection Integrity</p>
2	Voter is not presented with correct ballot information due to incorrect candidate identification.	Incorrect identification during candidate registration.	<p>Trusted candidate identification and registration are needed using:</p> <ul style="list-style-type: none"> - Security Procedures. - Best Practices. - Secure communications channels. - Authentication and identification of candidates <p>The candidate registration must follow standard Security Operating Procedures (SOPs) which ensure due diligence has been done.</p>
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. 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.	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. Before a vote is counted as a valid vote proof must be provided that the voter's secret data was present at the time of casting the vote.
		Any means of getting a legitimate voter to reveal his VToken data.	
6	Voting system impersonation	Inadequate authentication of registration system	Channel to provide: Point to point authentication
		Inadequate authentication of voting casting point (e.g. polling station/ballot box)	Channel to provide: Point to point authentication
7	Voter is not presented with correct ballot information	Inadequate integrity of the ballot information	Trusted path to voter on ballot options
		Given to the user	Integrity of the ballot information
		Held in the voting system	Integrity of cast votes
		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; Trojan horses Virus	Physical security
			Procedural security
			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 Procedures
		Multiple registration applications	Voter Identification
		Multiple allocation of voters credentials	Voter authentication
14	The vote cannot be altered from the voter's intention	Vulnerable client environment; Trojan horses Virus	Trusted path from voter's intent to vote record
			Vote integrity
			Vote non-repudiation
15	The vote may not be observed until the proper time	Votes may be observed before the end of the contest	Voter confidentiality
16	The voting system must be accountable and auditable		Non-repudiation of vote data.
			Audit tools

17	Identification and authentication information to and from the voter must be privacy protected	Loss of privacy	Channel to provide: Connection Confidentiality
18	The voter's actual identity may need to be anonymous	Voter's identification is revealed Denial of service attack	Voter's identification is anonymous
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.

942

Appendix B: The Timestamp Schema

943

Although used as part of EML, this schema has been put in a separate namespace as it is not an integral part of the language.

944

945

A time-stamp binds a date and time to the sealed data. The time-stamp seal also protects the integrity of the data.

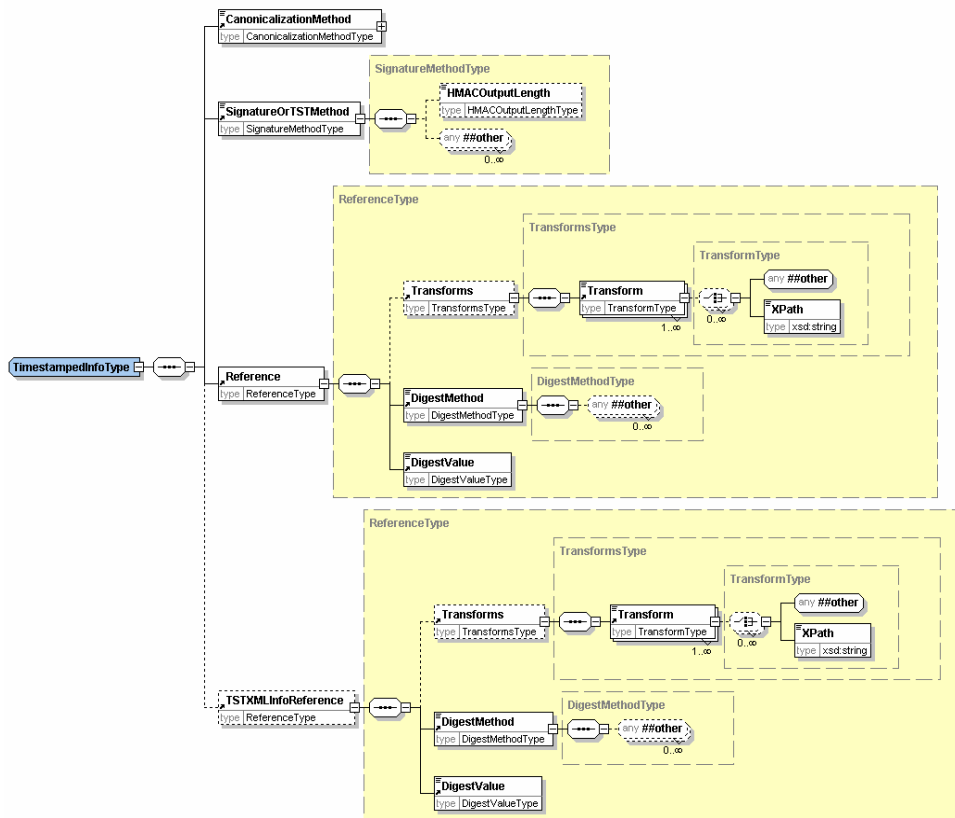
946

947

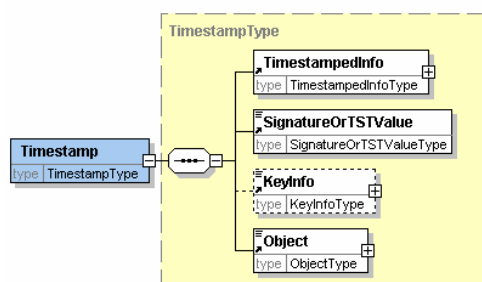
The structure of the time-stamp is similar to the structure of an XML Signature. The structure of the `Timestamp` element is shown here, followed by the detail of two of the four data types that

948

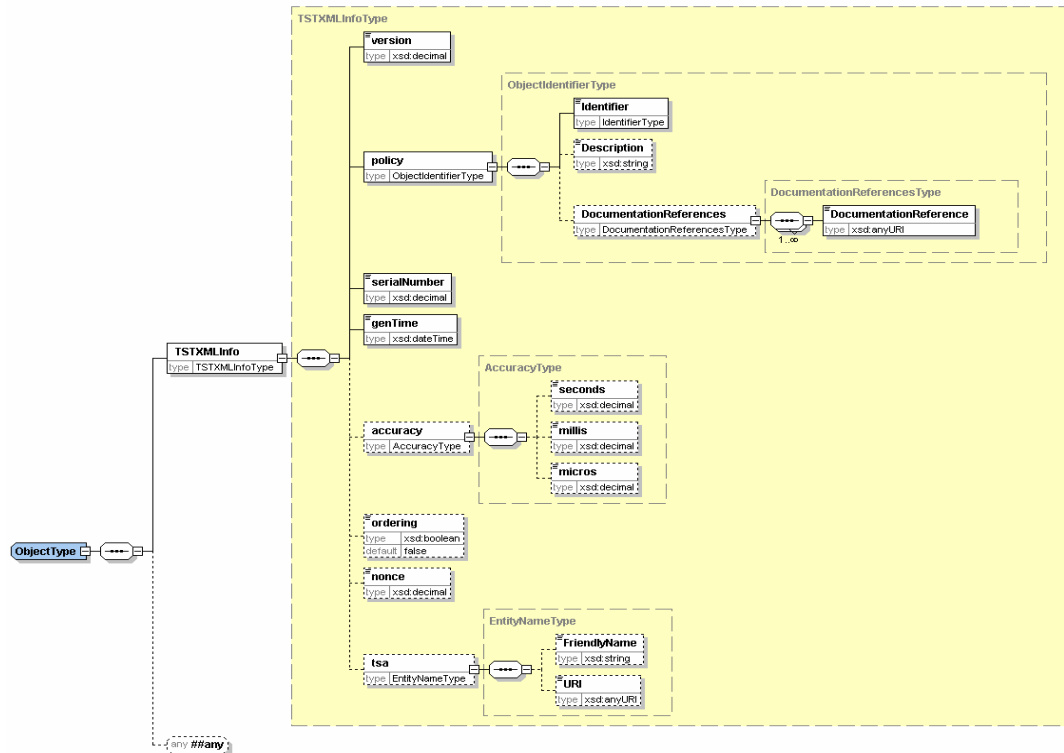
949



950



951



952

953 The timestamp structure may be used in one of two ways either:

- 954 • Using Internet RFC 3161 binary encoded time-stamp token with the time-stamp
- 955 information repeated in XML,
- 956 • Using a pure XML encoded time-stamp.

957 In the case of the RFC 3161 based time-stamp, the Timestamp structure is used as follows:

- 958 • within TimestampedInfo:
- 959 • TSTOrSignatureMethod identifies RFC 3161.
- 960 • Reference contains the URI reference of the voting data being time-stamped. The
- 961 DigestValue sub element contains the digest of the voting data being time-stamped.
- 962 • TSTXMLInfoReference is not present in this case.
- 963 • SignatureOrTSTValue holds the RFC 3161 time-stamp token applied to the digest of
- 964 TimestampedInfo. The TimestampedInfo is transformed to a canonical form using
- 965 the method identified in CanonicalizationMethod before the digest algorithm is
- 966 applied.
- 967 • KeyInfo contains any relevant certificate or key information.

968 Object contains the TSTXMLInfo element which is a copy of the information in
 969 SignatureOrTSTValue converted from RFC 3161 to XML encoding. The TSTXMLInfo
 970 element contains:

- 971 • the version of time-stamp token format. This would be set to version 1
- 972 • the time-stamping policy applied by the authority issuing the time-stamp,
- 973 • the time-stamp token serial number,
- 974 • the time that the token was issued, the contents of this element indicate the time of the
- 975 timestamp.

976 • optionally an indication as to whether the time-stamps are always issued in the order that
977 requests are received

978 • optionally a nonce¹ given in the request for the time-stamp token,

979 • optionally the identity of the time-stamping authority

980 In the case of a pure XML encoded time-stamp, the Timestamp structure is used as follows:

981 • within TimestampedInfo,

982 • TSTOrSignatureMethod identifies the algorithm used to create the signature value.

983 • Reference contains the URI reference of the voting data being time-stamped. The
984 DigestValue sub element contains the digest of the voting data being time-stamped.

985 • TSTXMLInfoReference must be present, and contains the URI reference of
986 TSTXMLInfo as contained within the Object element. The DigestValue sub element
987 contains the digest of the TSTXMLInfo.

988 • SignatureOrTSTValue contains the signature value calculated over the
989 TimestampedInfo using the signature algorithm identified in
990 TSTOrSignatureMethod having been transformed to a canonical form using the
991 method identified in CanonicalizationMethod. This signature is created by the time-
992 stamping authority.

993 • KeyInfo contains any relevant certificate or key information.

994 Object contains the XML encoded time-stamp information in an TSTXMLInfo element. The
995 contents of TSTXMLInfo is the similar as for the case described above. However, in this case the
996 information is directly signed by the time-stamping authority. The TSTXMLInfo element contains:

997 • version of time-stamp token format: This would be set to version 2

998 • the time-stamping policy applied by the authority issuing the time-stamp,

999 • the time-stamp token serial number,

1000 • the time that the token was issued, this is the time of the timestamp.

1001 • optionally an indication as to whether the time-stamps are always issued in the order that
1002 requests were received

1003 • optionally a nonce given in the request for the time-stamp token,

1004 • optionally the identity of the time-stamping authority.

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

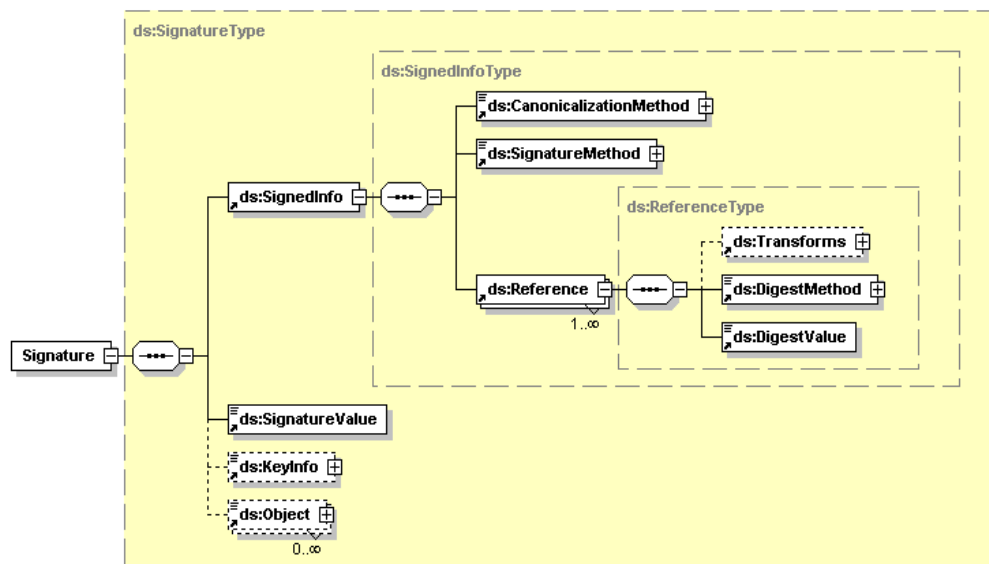
Appendix C: W3C XML Digital Signature

1005

1006 Some information on the digital signature is included here, but for full information refer to the
1007 Recommendation at [5].

1008 An XML Signature consists of:

- 1009 • `SignedInfo` which includes a sequence of references to the data being signed with the
1010 digest (eg. SHA-1 hash) of the data being signed
- 1011 • `SignatureValue` which contains the signature value calculated over the `SignedInfo`
1012 using the signature algorithm identified in `SignatureMethod` having been transformed
1013 to a canonical form using the method identified in `CanonicalizationMethod`
- 1014 • `KeyInfo` contains any relevant certificate or key information.
- 1015 • `Object` can contain any other information relevant to the signature



1016

Appendix D: Revision History

Rev	Date	What
V0.1a	2002-02-07	Draft e-voting schemas for internal comment
V0.2a	2002-02-13	Draft e-voting schemas for internal comment
V0.3a	2002-03-22	Draft e-voting schemas for public consultation comment
V0.4	2002-04-18	Draft Committee Specification version 2
V1.0	2002-04-29	Committee Specification for Technical Committee approval
V1.0	2002-05-13	Committee Specification
V2.0a	2002-06-13	Revised draft accommodating committee's comments
V2.0b	2002-07-15	Draft Committee Specification for Technical Committee approval
V2.0	2002-09-05	Committee Specification
V3.0a	2002-12-12	Draft Committee Specification
V3.0b	2003-02-06	Draft Committee Specification for Technical Committee approval
V3.0	2003-02-24	Committee Specification
V4.0a	2003-10-05	Revised draft accommodating requirements of Council of Europe Member States and UK pilots
V4.0b	2004-01-27	Draft Committee Specification
V4.0c	2004-03-09	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	Draft Committee Specification for Technical Committee approval.
V4.0	2005-01-24	Committee Specification

1019

References

- 1020 1. eXtensible Name and Address (XNAL) Specifications and Description Document (v2.0)
1021 Customer Information Quality Technical Committee OASIS July 2002 [http://www.oasis-
open.org/committees/tc_home.php?wg_abbrev=ciq](http://www.oasis-
1022 open.org/committees/tc_home.php?wg_abbrev=ciq)
- 1023 2. Address and Personal Details Fragment v1.1 Technology Policy Team, e-Government
1024 Unit, Cabinet Office UK, 1 March 2002
1025 http://www.govtalk.gov.uk/interoperability/draftschema_schema.asp?schemaid=92
- 1026 3. Extensible Markup Language (XML) 1.0 (Third Edition) Tim Bray et al, Worldwide Web
1027 Consortium, 4 February 2004 <http://www.w3.org/TR/REC-xml>
- 1028 4. XML-Signature Syntax and Processing Donald Eastlake et al, Worldwide Web
1029 Consortium, 12 February 2002 <http://www.w3.org/TR/xmlsig-core/>
- 1030 5. Voice Extensible Markup Language (VoiceXML) Version 2.0 Scott McGlashan et al
1031 Worldwide Web Consortium 16 March 2004 <http://www.w3.org/TR/voicexml20>

1032 Notices

1033 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
1034 that might be claimed to pertain to the implementation or use of the technology described in this
1035 document or the extent to which any license under such rights might or might not be available;
1036 neither does it represent that it has made any effort to identify any such rights. Information on
1037 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
1038 website. Copies of claims of rights made available for publication and any assurances of licenses
1039 to be made available, or the result of an attempt made to obtain a general license or permission
1040 for the use of such proprietary rights by implementors or users of this specification, can be
1041 obtained from the OASIS Executive Director.

1042 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
1043 applications, or other proprietary rights which may cover technology that may be required to
1044 implement this specification. Please address the information to the OASIS Executive Director.

1045 Copyright © OASIS Open 2005. *All Rights Reserved.*

1046 This document and translations of it may be copied and furnished to others, and derivative works
1047 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
1048 published and distributed, in whole or in part, without restriction of any kind, provided that the
1049 above copyright notice and this paragraph are included on all such copies and derivative works.
1050 However, this document itself does not be modified in any way, such as by removing the
1051 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS
1052 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
1053 Property Rights document must be followed, or as required to translate it into languages other
1054 than English.

1055 The limited permissions granted above are perpetual and will not be revoked by OASIS or its
1056 successors or assigns.

1057 This document and the information contained herein is provided on an "AS IS" basis and OASIS
1058 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO
1059 ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE
1060 ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A
1061 PARTICULAR PURPOSE.