

1 **DRAFT IEEE P1622™/D1 Standard for**
2 **Electronic Distribution of Blank**
3 **Ballots for Voting Systems**
4 **June 13, 2011**

5 Sponsor

6 **Standards Activities Board**
7 of the
8 **IEEE Computer Society**

9 Approved <XX MONTH 20XX>

10 **IEEE-SA Standards Board**

11
12 Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.
13 Three Park Avenue
14 New York, New York 10016-5997, USA

15 All rights reserved.

16 This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to
17 change. USE AT YOUR OWN RISK! Because this is an unapproved draft, this document must not be
18 utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards
19 Committee participants to reproduce this document for purposes of international standardization
20 consideration. Prior to adoption of this document, in whole or in part, by another standards development
21 organization, permission must first be obtained from the IEEE Standards Association Department
22 (stds.ipr@ieee.org). Other entities seeking permission to reproduce this document, in whole or in part, must
23 also obtain permission from the IEEE Standards Association Department.

24 IEEE Standards Association Department
25 445 Hoes Lane
26 Piscataway, NJ 08854, USA
27

Abstract: This standard specifies electronic data interchange formats for blank ballot distribution, primarily to satisfy the needs of the UOCAVA (Uniformed and Overseas Citizens Absentee Voting Act) and MOVE (Military and Overseas Voter Empowerment) Acts. Subsequent standards will address other requirements for electronic data interchange formats used by components of voting systems for exchange of electronic data. This scope does not include return of cast ballots by electronic means.

Keywords: Voting systems, vote-by-mail, overseas voters, military voters, UOCAVA, MOVE, EML, blank ballot distribution, elections.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA
Copyright © 20XX by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published <XX MONTH 20XX>. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-XXXX-XXXX-X STDXXXXX
Print: ISBN 978-0-XXXX-XXXX-X STDPDXXXXX

IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "AS IS."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

- 1 [Placeholder for legal language from OASIS regarding use of EML Version 7 by IEEE]

1 Introduction

2 This introduction is not part of IEEE P1622/D1, Draft Standard for Electronic Distribution of Blank Ballots for Voting
3 Systems.

4 Distributing blank paper ballots to overseas voters using conventional postal mail can involve considerable
5 delays, imperiling their timely return. To help overcome these barriers, Section 584 of the MOVE Act [1]
6 requires states to provide for military and overseas voters at least one electronic method for requesting and
7 receiving voter registration applications, absentee ballot requests and related election information. Also,
8 section 585 requires states to provide an electronic transmission method for the delivery of blank ballots.
9 This standard is intended to assist state and local election officials in making available electronic blank
10 ballots to voters in a manner directly akin to absentee voting. Specifically, this standard provides XML-
11 based data structures to be used for export of election information necessary to construct electronic blank
12 ballots.

13 Notice to users

14 Laws and regulations

15 Users of these documents should consult all applicable laws and regulations. Compliance with the
16 provisions of this standard does not imply compliance to any applicable regulatory requirements.
17 Implementers of the standard are responsible for observing or referring to the applicable regulatory
18 requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in
19 compliance with applicable laws, and these documents may not be construed as doing so.

20 Copyrights

21 This document is copyrighted by the IEEE. It is made available for a wide variety of both public and
22 private uses. These include both use, by reference, in laws and regulations, and use in private self-
23 regulation, standardization, and the promotion of engineering practices and methods. By making this
24 document available for use and adoption by public authorities and private users, the IEEE does not waive
25 any rights in copyright to this document.

26 Updating of IEEE documents

27 Users of IEEE standards should be aware that these documents may be superseded at any time by the
28 issuance of new editions or may be amended from time to time through the issuance of amendments,
29 corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the
30 document together with any amendments, corrigenda, or errata then in effect. In order to determine whether
31 a given document is the current edition and whether it has been amended through the issuance of
32 amendments, corrigenda, or errata, visit the IEEE Standards Association web site at
33 <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

34 For more information about the IEEE Standards Association or the IEEE standards development process,
35 visit the IEEE-SA web site at <http://standards.ieee.org>.

36 Errata

37 Errata, if any, for this and all other standards can be accessed at the following URL:
38 <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL
39 for errata periodically.

1 Interpretations

2 Current interpretations can be accessed at the following URL: [http://standards.ieee.org/reading/ieee/interp/](http://standards.ieee.org/reading/ieee/interp/index.html)
 3 [index.html](http://standards.ieee.org/reading/ieee/interp/index.html).

4 Patents

5 *[If the IEEE has not received letters of assurance prior to the time of publication, the following notice*
 6 *shall appear:]*

7 Attention is called to the possibility that implementation of this standard may require use of subject matter
 8 covered by patent rights. By publication of this standard, no position is taken with respect to the existence
 9 or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying
 10 Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity
 11 or scope of Patents Claims or determining whether any licensing terms or conditions provided in
 12 connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable
 13 or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any
 14 patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further
 15 information may be obtained from the IEEE Standards Association.

16 *[The following notice shall appear when the IEEE receives assurance from a known patent holder or*
 17 *patent applicant prior to the time of publication that a license will be made available to all applicants*
 18 *either without compensation or under reasonable rates, terms, and conditions that are demonstrably free*
 19 *of any unfair discrimination.]*

20 Attention is called to the possibility that implementation of this standard may require use of subject matter
 21 covered by patent rights. By publication of this standard, no position is taken with respect to the existence
 22 or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a
 23 statement of assurance that it will grant licenses under these rights without compensation or under
 24 reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair
 25 discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for
 26 which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential
 27 Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope
 28 of Patents Claims, or determining whether any licensing terms or conditions provided in connection with
 29 submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-
 30 discriminatory. Users of this standard are expressly advised that determination of the validity of any patent
 31 rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information
 32 may be obtained from the IEEE Standards Association.

33

1 Participants

2 At the time this draft standard was submitted to the IEEE-SA Standards Board for approval, P1622
3 Working Group had the following membership:

4 Arthur M. Keller, *Chair*
5 Stephen Berger, *Vice Chair*
6 John P. Wack, *Vice Chair, Editor*
7 Carmelo Montanez-Rivera, *Secretary*
8
9

10 Participant1	13 Participant4	16 Participant7
11 Participant2	14 Participant5	17 Participant8
12 Participant3	15 Participant6	18 Participant9

19
20
21 The following members of the individual balloting committee voted on this standard. Balloters may have
22 voted for approval, disapproval, or abstention.
23

24 *(to be supplied by IEEE)*
25

26 Balloter1	29 Balloter4	32 Balloter7
27 Balloter2	30 Balloter5	33 Balloter8
28 Balloter3	31 Balloter6	34 Balloter9

35
36
37 When the IEEE-SA Standards Board approved this standard on <XX XXXX 2011>, it had the following
38 membership:

39 *(to be supplied by IEEE)*
40

41 <Name>, *Chair*
42 <Name>, *Vice Chair*
43 <Name>, *Past President*
44 <Name>, *Secretary*

45 SBMember1	48 SBMember4	51 SBMember7
46 SBMember2	49 SBMember5	52 SBMember8
47 SBMember3	50 SBMember6	53 SBMember9

54 *Member Emeritus

55
56
57 Also included are the following nonvoting IEEE-SA Standards Board liaisons:

58 <Name>, *NRC Representative*
59 <Name>, *DOE Representative*
60 <Name>, *NIST Representative*
61

62 <Name>
63 *IEEE Standards Program Manager, Document Development*
64

65 <Name>
66 *IEEE Standards Program Manager, Technical Program Development*
67
68

1 Contents

2	1. Normative references.....	1
3	2. Definitions	2
4	3. Version	4
5	4. Goal	4
6	5. Summary	4
7	6. Actors	5
8	7. Stakeholders	6
9	8. Pre-conditions/Assumptions	6
10	9. Main scenario	6
11	10. High-level election data requirements	8
12	11. Additional notes.....	8
13	Annex A – Files included in this standard.....	10
14	Annex B – The EML 505 schema and file	11
15	Annex C discusses using the EML 505 file to point to electronic blank ballots located externally.	11
16	Annex C – EML 505 example using pre-constructed electronic blank ballots.....	13
17	Annex D - Using other base EML schemas.....	15
18	Annex E – Use of EML 330 and 470 for ballot tracking.....	17
19	Annex F - Example of using the SEAL digital signature structure	21
20		

Draft IEEE P1622™/D1 Standard for Electronic Distribution of Blank Ballots for Voting Systems

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

- [1] Military and Overseas Voter Empowerment (MOVE) Act, 2010, [http://ballotpedia.org/wiki/index.php/Military_and_Overseas_Voter_Empowerment_\(MOVE\)_Act](http://ballotpedia.org/wiki/index.php/Military_and_Overseas_Voter_Empowerment_(MOVE)_Act)
- [2] OASIS Election Markup Language (EML), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election,
- [3] OASIS EML v7 draft, June 2011, contains v7 package of schemas and example files described in this standard, http://www.oasis-open.org/committees/document.php?document_id=42511&wg_abbrev=election
- [4] TGDC Recommendations of 2007, U.S. Election Assistance Commission, August 1, 2007, http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.

- 1 [5] Uniformed and Overseas Citizens Absentee Voting Act as amended by the MOVE Act, 2010,
2 <http://www.fvap.gov/resources/media/uocavalaw.pdf>.
- 3
- 4 [6] Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes, U.S.
5 Election Assistance Commission, April 6, 2011,
6 http://www.eac.gov/assets/1/Documents/UOCAVA_Registration_and_Voting_Processes.pdf.
- 7
- 8 [7] Voting Information Project (VIP), PEW Center on the States,
9 http://www.pewcenteronthestates.org/uploadedFiles/Voting_Information_Project_brief.pdf
- 10
- 11 [8] Voluntary Voting System Guidelines Version 1.0, U.S. Election Assistance Commission, 2005,
12 http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.
- 13
- 14 [9] XML Signature Syntax and Processing (Second Edition), W3C Recommendation June 10, 2008,
15 <http://www.w3.org/TR/xmlsig-core/>.
- 16

17 2. Definitions

18 For the purposes of this document, the following terms and their definitions apply. The *IEEE Standards*
19 *Dictionary: Glossary of Terms & Definitions* should be consulted for terms not defined in this clause.¹ The
20 terms here are from [4], which contains an updated version of terms and definitions from [8] that have been
21 vetted with election officials for common usage and precision. These definitions make reference to other
22 terms defined in this section; where this occurs the terms are underlined.

23 **blank ballot** - votable presentation of every contest included in a particular ballot style. Discussion: the
24 ballot presentation could be a collection of one or more pieces of paper or an electronic representation such
25 as a PDF document or JPG image.

26 **ballot configuration** - set of contests in which voters of a particular group (e.g., political party and/or
27 election district) are entitled to vote.

28 **ballot rotation** - process of varying the order of the contest choices within a given contest.

29 **ballot style** - concrete presentation of a particular ballot configuration. Discussion: A given ballot
30 configuration may be realized by multiple ballot styles, which may differ in the language used, the ordering
31 of contests and contest choices, etc. The ballot configuration also observes all state/local presentation
32 (formatting) rules.

33 **BBD** - Blank Ballot Distribution.

34 **BDS** - Ballot Delivery System, used to denote an Internet-accessible system used by overseas voters to
35 obtain electronic blank ballots.

36 **contest** - (1) a single decision being put before the voters (e.g., the selection of candidates to fill a
37 particular public office or the approval or disapproval of a constitutional amendment). Discussion: This
38 term subsumes other terms such as "race," "question," and "issue" that are sometimes used to refer to
39 specific kinds of contests. (2) subdivision of a ballot pertaining to a single decision being put before the
40 voters.

¹ The *IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.

- 1 **EAC** - The U.S. Election Assistance Commission, <http://www.eac.gov>.
- 2 **election district** - administrative division in which voters are entitled to vote in contests that are specific to
- 3 that division, such as those for state senators and delegates. Discussion: An election district may overlap
- 4 multiple precincts, and a precinct may overlap multiple election districts (see [split precinct](#)).
- 5 **electronic blank ballot** - digital blank ballot generated by election officials that observe all state/local
- 6 formatting rules and is considered a valid legal ballot. For example, a PDF blank ballot intended to be a
- 7 printed as a paper ballot is a votable electronic blank ballot. A finer distinction is “electronic blank ballot
- 8 document,” however “document” is assumed in “electronic blank ballot.”
- 9 **EML** - Election Markup Language, see [2].
- 10 **EMS** - Election Management System.
- 11 **EO** - state or local Election Official, possibly in conjunction with [FVAP](#).
- 12 **FVAP** - The Federal Voting Assistance Program, part of the U.S. Department of Defense,
- 13 <http://www.fvap.gov>.
- 14 **FWAB** - Federal Write-In Absentee Ballot.
- 15 **OASIS** - Organization for the Advancement of Structured Information Standards, [http://www.oasis-](http://www.oasis-open.org)
- 16 [open.org](http://www.oasis-open.org).
- 17 **ordered ballot configuration** – a [ballot configuration](#) with (a) ordering information regarding how
- 18 [contests](#) must appear in a [ballot style](#) and (b) the [vote variation](#) associated with each [contest](#).
- 19 **NIST** - The U.S. National Institute of Standards and Technology, <http://www.nist.gov>.
- 20 **overseas voter** – A U.S. citizen eligible to vote and residing overseas, whether on active military duty or
- 21 living abroad.
- 22 **schema** – an [XML](#) file containing definitions of data elements and attributes with rules for usage.
- 23 **split precinct** - precinct serving voters from two or more administrative divisions, such as [election districts](#),
- 24 that may require different [ballot configurations](#).
- 25 **UML** - Unified Modeling Language.
- 26 **UOCAVA** - The Uniformed and Overseas Citizens Absentee Voting Act, see [5], [6].
- 27 **UOCAVA voter** – see [overseas voter](#).
- 28 **voting variation** - voting style, option, or feature such as in-person voting, absentee voting, provisional /
- 29 challenged ballots, review-required ballots, closed primaries, open primaries, write-ins, ballot rotation,
- 30 straight party voting, cross-party endorsement, split precincts, N-of-M voting, cumulative voting, or ranked
- 31 order voting.
- 32 **VRDB** – Voter Registration Database.
- 33 **XML** - Extensible Markup Language.
- 34

3. Version

Version: June 13, 2011

4. Goal

The goal of this standard is to assist the Federal Voting Assistance Program (FVAP) and U.S. States and Territories and the District of Columbia in achieving the goals of the Uniformed and Overseas Citizens Absentee Voting Act [5], [6] (UOCAVA) and the Military and Overseas Voter Empowerment (MOVE) Act [1], i.e., to assist overseas military and citizens in participating fully in US elections. This standard, in general, serves the purpose of electronic distribution of blank ballots to uniformed and overseas voters, which can significantly improve timely access to blank ballots. This standard provides export formats for the election information needed to facilitate construction and delivery of electronic blank ballots to Internet-accessible ballot delivery systems (BDSs). While this standard is intended for use primarily by FVAP and state and local election officials (EOs) from U.S. States and Territories and the District of Columbia, it may also be useful in achieving other goals, such as permitting consistent export of information between voter registration database systems (VRDBs) and BDSs. This standard may also be referenced or subsumed by other standards in the future (e.g., a standard for remote voting purposes).

5. Summary

This standard assists FVAP and EOs in making available electronic blank ballots to voters that can be downloaded from a BDS and then printed and returned and processed in a manner directly akin to absentee voting. Specifically, it provides XML schemas and examples in OASIS Election Markup Language [2] (EML) for the purposes of exporting from VRDBs and Election Management Systems (EMS), in a common XML format, the jurisdictional information and ballot definition information needed to facilitate automated construction of electronic blank ballots. It also provides the opportunity for overseas voters to track the status of their ballot, as required in the MOVE Act [1]. This standard is only for the creation of electronic blank ballots and does not make provisions for the electronic return of those ballots, nor for verifying a voter's entitlement to vote.

NOTE: *To facilitate understanding, this standard references the EML 505 schema throughout as the default data source for base line information content purposes. The EML 505 has been optimized to make it convenient to use with the PEW Foundation's Voter Information Project [7] (VIP), which assists voters in finding their voting locations and showing the contests/issues on their ballot. Use of the EML 505 is not mandated; other base EML schemas that provide the same data structures as found in the EML 505 schema could be employed instead or in addition; for details see Annex D.*

The EML 505 file can be built to serve two basic purposes: (a) for use in indexing from overseas voters' jurisdictional information to their corresponding electronic blank ballots which may be pre-constructed prior to the election and stored externally, or (b) for use in dynamic constructing of generically-formatted blank ballots, minus state-specific formatting details. In the case of (b), the state-specific formatting details would presumably be supplied by the BDS. This standard provides for both purposes, as follows:

Pre-Election:

- a) If pre-constructing electronic blank ballots (e.g., PDF files) that can later be presented to voters by BDSs, then export of certain jurisdictional and election information to an EML 505 and the appropriate linkage to the jurisdiction's ballots stored elsewhere (e.g. a collection of PDF blank ballot files).

- b) If BDSs are dynamically constructing electronic blank ballots (or FWABs), then export of certain jurisdictional and election information and ballot definition information to an EML 505 file. For example, an EML 505 file can be built to be a repository of ordered ballot configurations linked with their corresponding elections and precincts/voting locations. As noted, this does not include state-specific formatting details on the ballot.

During voting:

- a) Presentation of the electronic blank ballot to the voter according to the following:
 - 1) Pre-constructed electronic blank ballot: Mapping of the voter's registration address (and political party for certain primary elections) to jurisdictional information stored within an EML 505 file that is indexed to an externally-stored electronic blank ballot.
 - 2) Dynamically-constructed electronic blank ballot (or FWAB): Matching of the voter's registration address (and political party for certain primary elections) to jurisdictional information stored within an EML 505 file and then to the ordered ballot configuration stored in the same file. Then, dynamic construction of the electronic blank ballot using state-specific presentation/formatting details provided externally (e.g., by applications).

The next step could include either the voter printing the ballot document for hand-marking or, potentially, the voter marking selections on the electronic blank ballot and then printing it with the selections already marked, e.g., a fillable PDF.

Additionally, the MOVE Act [1] requires that an overseas voter be able to determine whether their ballot has been received by the appropriate EO. This standard provides for this ballot tracking by use of the EML 330 Election List schema and the EML 470 Voter Token Log schema, as follows:

- a) Export of overseas voter information from the VRDB to the EML 330, and then transmission of the EML 330 to the BDS. The EML 330 contains elements to show ballot status, which are initially empty.
- b) When voters use the BDS to access ballots, transmission of an EML 470 with ballot status information, e.g., issued, back to the jurisdiction, which may then update the VRDB.
- c) As ballots are received at the jurisdiction, exports from the VRDB to the EML 330, with information updated to show that certain ballots have been received. Then, transmission of the EML 330 back to the BDS, which may then provide appropriate overseas voters with status information, e.g., ballot accepted.

6. Actors

There are two primary actors for this standard:

- a) The overseas voter, who requests and retrieves a blank ballot, and
- b) The EO (state/local or FVAP), who prepares ballot information beforehand and receives the returned ballot from the overseas voter.

7. Stakeholders

Primary stakeholders for this standard include

- EOs in US States,
- The Federal Voting Assistance Program (FVAP) in implementing the UOCAVA [6] and MOVE Act [1], and
- Overseas voters including military and citizens stationed or residing abroad.

8. Pre-conditions/Assumptions

There are a number of basic pre-conditions and assumptions for this standard. Assumptions include the following:

- a) Overseas voters will have sufficient Internet connectivity to BDSs.
- b) Overseas voters will be able to locate and successfully retrieve ballots from their respective jurisdictions using installed software on their client systems.
- c) Overseas voters will be able to print the ballots successfully and mail them using envelopes provided for mailing to their jurisdictions or some other postal site.

Preconditions are primarily those items pertaining to voter authentication information and ballot setup. These would include:

- a) Exports from VRDBs of voter registration data and jurisdictional data for overseas voters for the purposes of identifying each voter and presenting the correct ballot.
- b) Exports from EMSs (for both jurisdiction data and ballot description data) for construction of the ballot.
- c) If electronic blank ballots are to be created before the election and stored for later retrieval by overseas voters, then preparation of the electronic blank ballots and storage in BDSs.
- d) If electronic blank ballots are to be created dynamically during voting, then BDSs with capability to add state-specific formatting/presentation details to the displayed ballot.

9. Main scenario

The main scenario (for which this standard has been created) outlines those activities of the actors that involve the exchange of the election information supporting the presentation of a blank ballot to a voter, using the accompanying EML 505 schema as a reference. There are two primary actors in this standard: the overseas voter and the EO. The EO is engaged in those activities that result in the construction of electronic blank ballots and in receiving returned paper ballots from the overseas voter and then in performing subsequent status updates and tabulations. The overseas voter is engaged in requesting a ballot, marking/printing the ballot, and mailing it to the voter's respective jurisdiction (or other designated postal site).

The steps below outline the activities of the EO:

a) The EO exports registration information about overseas voters from the VRDB into an EML 330 Election List file, including voter name, registered address, and details about party affiliation and ballot type. The EO sends this to the BDS for use in establishing the list of overseas voters and their particulars that should be permitted to connect to the BDS to download ballots. Periodically during the election, EOs could refresh the BDS with EML 330 exports as overseas voters are added, modified, or deleted from the VRDB.

b) The EO exports election data from the VRDB/other databases and the EMS into an EML 505 file. The EO sends the data to the BDS, which can use it to locate elections for which overseas voters are eligible to participate and the corresponding ballots. The election data would include:

- 1) jurisdictional information,
- 2) street segment data (as needed),
- 3) ballot definitions and race/candidate information for each ballot style (as needed), and
- 4) corresponding ballot styles (as needed).

If the BDS will be retrieving pre-constructed electronic blank ballots (and not building them dynamically), the EML 505 file would be populated with the information necessary to find voters' precincts and corresponding election information and indices to externally-located electronic blank ballots. Accordingly, this could involve items 1) and possibly 2), above.

c) When a voter downloads an electronic blank ballot from the BDS, the BDS sends an EML 470 Voter Token Log file to the voter's corresponding EO, indicating that the voter has downloaded a certain ballot.

d) The EO receives printed ballots as they are returned by voters via postal mail. The processing of these ballots is comparable to that of processing absentee/provisional ballots. The EO updates the VRDB with status regarding the received ballots, e.g., ballot accepted, rejected.

e) Periodically, the EO makes periodic exports of this status information from the VRDB to an EML 330 file, and uses this to refresh the BDS. The BDS updates the corresponding overseas voters with the status of their received ballots.

The steps below outline the activities of the overseas voter:

f) An overseas voter uses a BDS to enter information about themselves, e.g., their name, address, etc., which can then be used to identify the voter and determine whether the voter is eligible to vote in the election at hand and retrieve an electronic blank ballot.

g) If the voter is eligible to vote in the election, the voter downloads their ballot (making choices among party ballot styles if necessary).

- h) The voter may potentially make ballot selections among the candidates and then print a marked paper ballot or, if ballot marking is not available or desired, print the ballot and mark it by hand.
- i) The voter then places the paper ballot in an envelope provided. The voter may also include a signed declaration form attesting that the voter is who they purport to be and that they are eligible to vote in the election.
- j) The voter mails the paper ballot to the EO or to some other designated postal site.
- k) According to the Move Act [1], the voter can check on the status of their received ballot, e.g., receive e-mail updates from the BDS regarding the status of the voter's received ballot.

Figure 1 models these steps from the perspectives of the overseas voter and the EO. This model shows only the major steps involved in this scenario; it does not purport to be a comprehensive process diagram.

10. High-level election data requirements

Following is a high-level list of the election data required for this standard:

- a) Voter registration data and voter ballot status, exported into an EML 330 Election List file.
- b) Election jurisdiction data to provide mapping from voter registration data to voting precincts, exported into an EML 505 file. This may include hierarchical jurisdiction information such as street segment information.
- c) Further mapping from precincts to pre-configured ballots or to election information necessary to construct a generically formatted ballot, including candidates, contests, and contest rules and ordering information on the ballot.

Other information necessary but supplied externally to this standard include:

- d) Election display rules, i.e., how the ballot must appear on the screen or how the ballot must appear in print.
- e) Ballot returns data such as the address where ballots are to be returned or drop shipment data.

11. Additional notes

Electronic return of voted ballots is not described by this standard. However, such a system would necessarily involve the data as required by this standard and additional data.

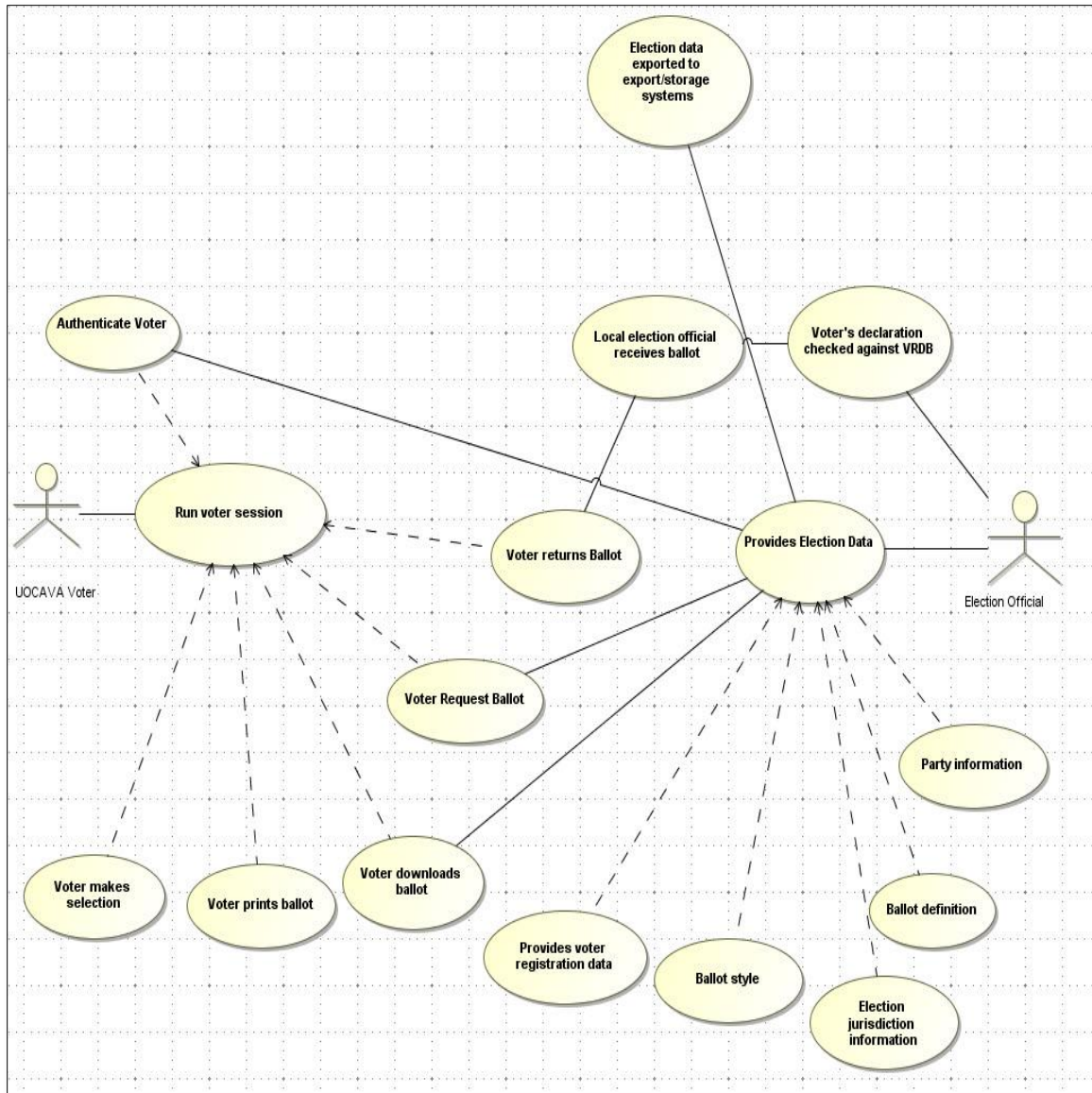


Figure 1 – Blank ballot distribution data model

1 **Annex A – Files included in this standard**

2 The EML draft version 7 package is located at [3] and includes the UOCAVA-BBD example files referred
 3 to throughout this standard in the *samples/UOCAVA* subdirectory. The following files are included:

- 4 — UOCACA-BBD-example-EML330-*date*.xml
- 5 — UOCACA-BBD-example-EML330u-*date*.xml
- 6 — UOCACA-BBD-example-EML410-*date*.xml
- 7 — UOCACA-BBD-example-EML470-*date*.xml
- 8 — UOCACA-BBD-example-EML505-*date*.xml (shares the same contest data as in UOCACA-BBD-
 9 example-EML410-*date*.xml)
- 10 — UOCACA-BBD-example-EML470WithSeal-*date*.xml (contains an EML SEAL structure with the
 11 file's digital signature information)
- 12 — UOCACA-BBD-example-ballot-F2Z666-*date*.pdf (can be generated from EML 410 or 505 files)
- 13 — UOCACA-BBD-example-ballot-F3Y111-*date*.pdf (can be generated from EML 410 or 505 files)

14
 15 where *date* is MMDDYYYY, such that “06012011” is June 1, 2011.

16 The package also includes a subdirectory *samples/VIP* containing examples of Virginia 2010 VIP [7] files
 17 and an XSLT transform that includes parameters to control the generation of EML 150 and EML 505 street
 18 segment data, as well as automatically producing the EML 110 Election Event, 230 Candidate List, and 505
 19 files.

1 **Annex B – The EML 505 schema and file**

2 The EML 505 schema was designed for this standard and for general use in creating electronic blank
 3 ballots for overseas voters. The 505 schema is composed of XML structures found also in other base EML
 4 schemas, however it has been optimized to make it convenient to use with the PEW Foundation's Voter
 5 Information Project [7] (VIP), which assists voters in finding their voting locations and showing the
 6 contests/issues on their ballot.

7 Use of the EML 505 is not mandated, however, other base EML schemas that provide the same data
 8 structures as found in the EML 505 schema could be employed instead or in addition (see Annex D for
 9 information regarding the other base EML schemas).

10 Figure B-1 shows a high-level view of the EML 505 structure. The EML 505 schema contains two major
 11 components:

- 12 a) A structure that describes various election authority details
- 13 b) A series of linked structures that describe information on
 - 14 1) voting location information (localities, locality boundaries, districts, polling
 - 15 locations),
 - 16 2) information on the elections in each precinct,
 - 17 3) contests and propositions in corresponding elections including vote variation
 - 18 information and the order in which the contests appear on the ballot, and
 - 19 candidates in the contests.

20
 21 The election information and linked structures are populated from exports from the VRDB and EMS. The
 22 contest information links to a ballot ID, which can be used by a BDS for either of the following:

- 23
- 24 a) For dynamically constructing the ballot with the election and contest information
- 25 contained in the EML 505 file, or
- 26 b) For pointing to a pre-constructed electronic blank ballot located elsewhere.

27
 28 Accordingly, the voting location information in an EML 505 file will point to contests, propositions, and
 29 candidates, which will point to a ballot ID. For pointing to pre-constructed electronic blank ballots located
 30 elsewhere, the ballot ID can be loaded with an identifier of the ballot or a URL to its location. An example
 31 EML 505 file for the purposes of dynamic ballot construction is included with this standard (UOCAVA-
 32 BBD-example-EML505-date.xml), along with two example ballots built from the information in the file
 33 (UOCAVA-BBD-example-ballot-F2Z666-date.pdf and UOCAVA-BBD-example-ballot-F3Y111-
 34 date.pdf).

35
 36 Annex C discusses using the EML 505 file to point to electronic blank ballots located externally.

37

38

39

40

41

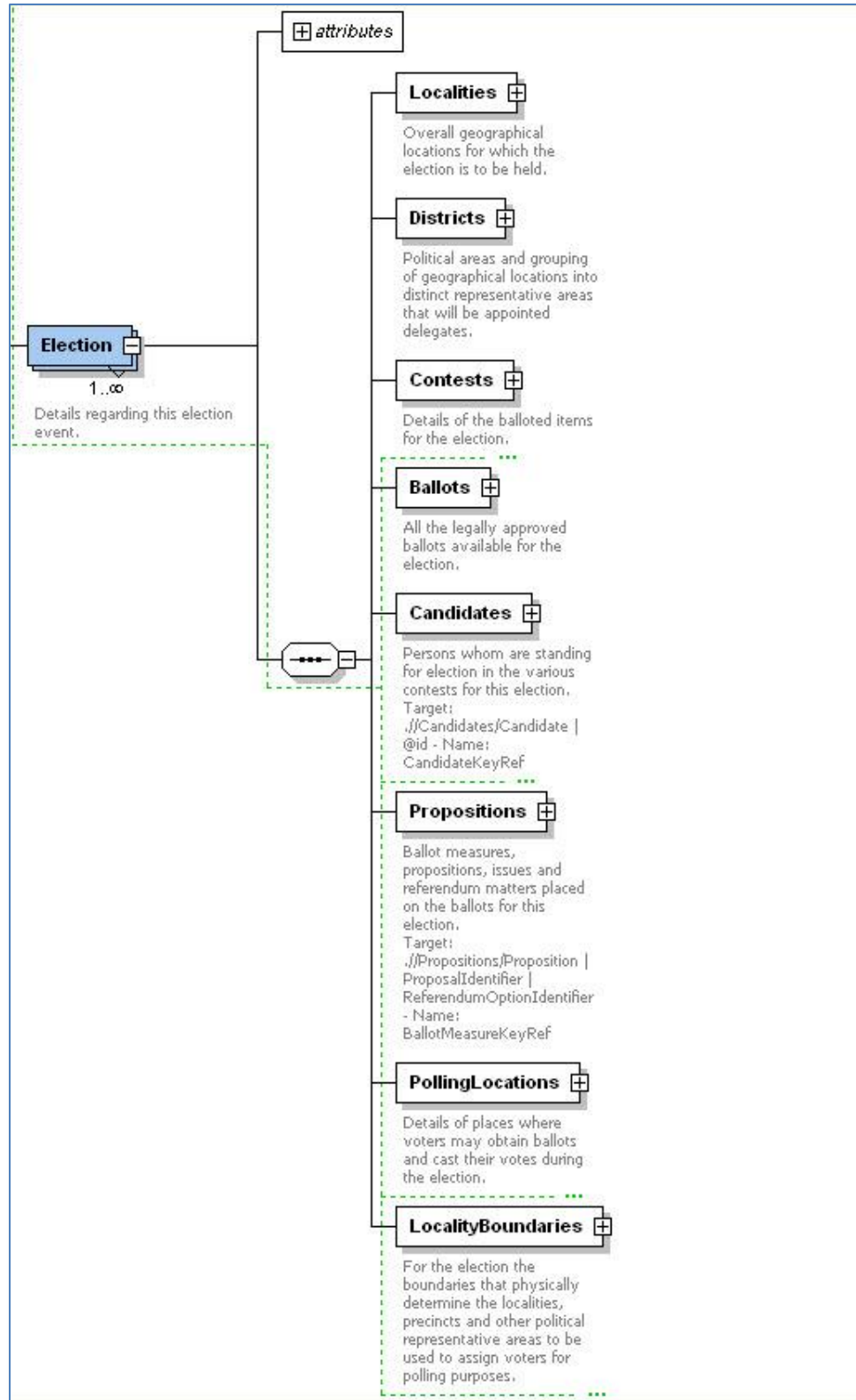


Figure B-1 – EML 505 main structures

Annex C – EML 505 example using pre-constructed electronic blank ballots

As described in Annex B, an EML 505 file can be used generally one of two ways:

- a) For dynamically constructing the ballot with information contained in an EML 505 file, or
- b) For pointing to a pre-constructed electronic blank ballot located elsewhere:
 - 1) by identifying an externally-located ballot by an associated ID number, or
 - 2) by pointing to a URL where an image of actual ballot can be retrieved.

This annex shows examples for pointing to pre-constructed electronic blank ballots. Figure C-1 below shows the portion of the EML 505 schema that identifies a ballot.

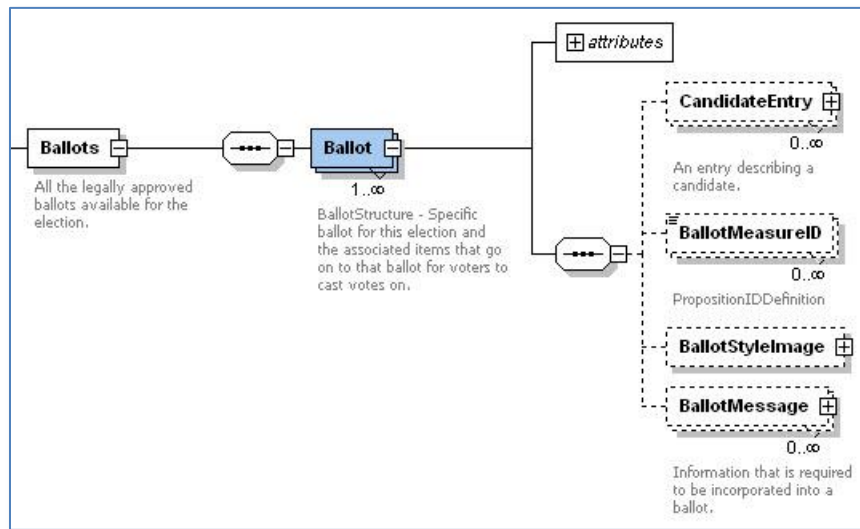


Figure C-1 – EML 505 schema location of ballot structure

Figure C-2 is an XML file instance of this portion of the schema. The `<Ballot id>` field could be used to identify a corresponding electronic blank ballot stored externally. In Figure C-2, the ID is “F3Y111,” which could be used to index to the corresponding electronic blank ballot located in, e.g., a data store of PDF files.

```

</Ballot>
<Ballot id="F3Y111">
  <CandidateEntry><CandidateIdentifier IdNumber="2B234"><CandidateName>Henry A. Benson</CandidateName>
    <KnownAs>H Benson</KnownAs><ShortCode>2b1</ShortCode><IsWriteIn>>false</IsWriteIn></CandidateIdentifier>
    <CandidateURL>HenryABensonSenateCampaign.org</CandidateURL>
  </CandidateEntry>
  <CandidateEntry><CandidateIdentifier IdNumber="2B235"><CandidateName>Robert Burck</CandidateName>
    <ShortCode>2b2</ShortCode><IsWriteIn>>false</IsWriteIn></CandidateIdentifier><CandidateURL>RobertBurk.org</CandidateURL>
  </CandidateEntry>
  <CandidateEntry>
    <CandidateIdentifier IdNumber="2B236"><CandidateName>Kevin B. Zeese</CandidateName><ShortCode>2b3</ShortCode>
    <IsWriteIn>>false</IsWriteIn></CandidateIdentifier><CandidateURL>KBZPAC.com</CandidateURL>
  </CandidateEntry>
  <BallotStyleImage>
    <URL Checksum="adfc7068f44947aab2e296952e87711dfc614e769643a42b31449e9ec95ccf2b"
    HashAlgorithm="SHA-256" HMAC="hex" MimeType="pdf">http://www.AK.gov/ballots/F3Y111.htm
    </URL>
  </BallotStyleImage>
  <BallotMessage>
    <Message DisplayOrder="1" Format="text" Seqn="0" Lang="en-us" MimeType="text">
      This is a blank ballot for the State Contests for the November 8, 2011 General Election in the State of Alaska</Message>
    <Message DisplayOrder="2" Format="text" Seqn="0" Lang="en-us" MimeType="text">
      [This ballot is for voters in District X for the State Senate for the State of Alaska</Message>
    </BallotMessage>
  </Ballot>

```

Figure C-2 – Excerpt from EML 505 file “UOCAVA-BBD-example-EML505-date.xml”

Figure C-2 also shows a `<BallotStyleImageURL>` element. Its value is a pointer to a ballot image located at the fictional URL “<http://www.AK.gov/ballots/F3Y111.htm>.” A BDS could also use this URL to access the ballot and subsequently display it to an overseas voter.

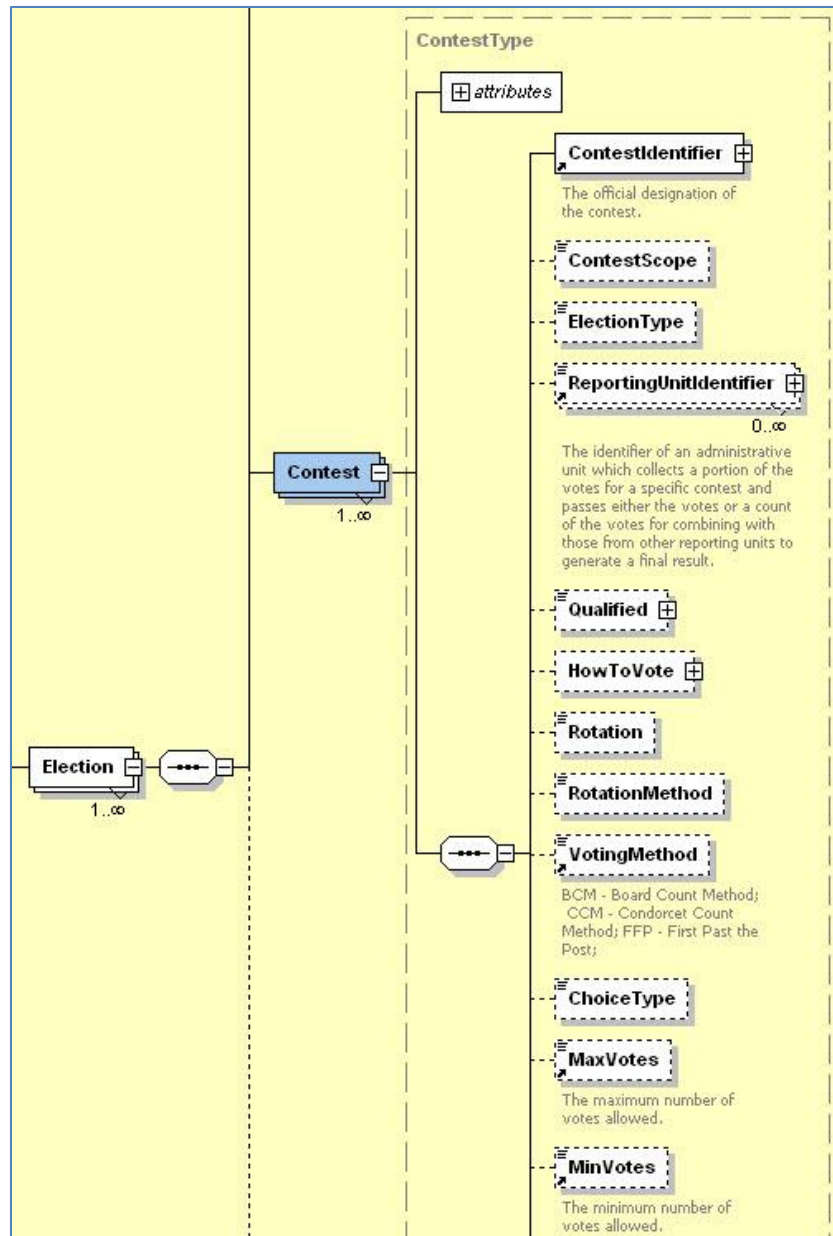
In the example, the `<BallotStyleImageURL>` element also shows optional fields for containing a digital signature of the ballot image. The EML 505 (and EML 410) example contains ballot information to build two example ballots (UOCAVA-BBD-example-ballot-F2Z666-date.pdf and UOCAVA-BBD-example-ballot-F3Y111-date.pdf). The actual digital signatures of the example ballots generated by this 505 file are stored in the file’s `<BallotStyleImageURL>` elements.

1 Annex D - Using other base EML schemas

2 As stated in Annex B, use of the EML 505 is not mandated; other base EML schemas that provide the same
 3 data structures as found in the EML 505 schema could be employed instead or in addition. The other base
 4 EML schemas that contain the same structures as in the EML 505 schema are:

- 5 — EML 110 Election Event: structures dealing with information about the elections
- 6 — EML 230 Candidate List: structures for contests and candidates on the contests
- 7 — EML 410 Ballot List: structures for the actual ballots used for the elections

8



9

10 **Figure D-1 – The EML 410 contest structure**

The contest structure of the EML 410 is shown in Figure D-1. This standard includes an example EML 410 file (UOCAVA-BBD-example-EML410-*date.xml*) whose contest structure information was used also in the example EML 505 file (UOCAVA-BBD-example-EML505-*date.xml*). The EML 410 (and 505) example contains ballot information to build two example ballots (UOCAVA-BBD-example-ballot-F2Z666-*date.pdf* and UOCAVA-BBD-example-ballot-F3Y111-*date.pdf*).

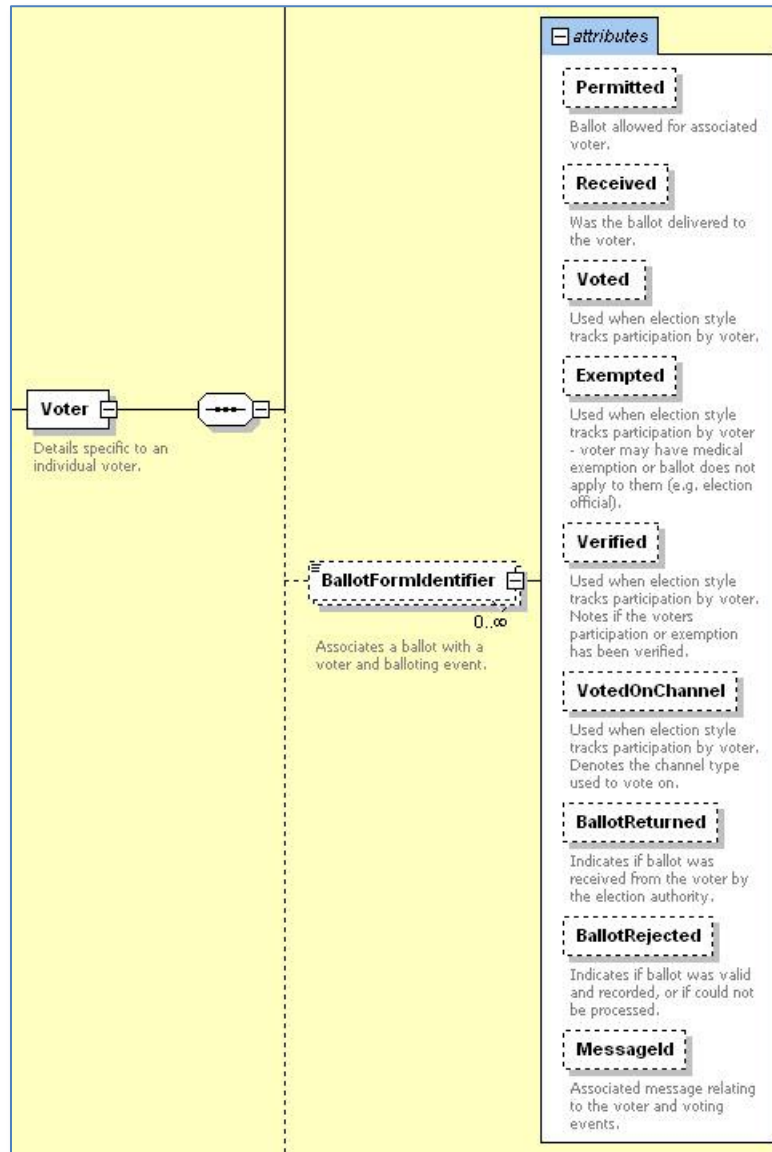
General Election for Home County AK Home County AK	
General Election for Home County AK	
US President Vote for no more than one	
☐	Theodore Roosevelt Republican
☐	Harry S. Truman Democrat
☐	George Washington Constitutional Reform
US Congress District 2 Vote for no more than one	
☐	Joseph Gurney Cannon Republican
☐	Frederick Muhlenberg Federalist
☐	Samuel J. Randall Democrat

Figure D-2 – Example ballot built from UOCAVA-BBD-example-EML410-*date.xml* or UOCAVA-BBD-example-EML505-*date.xml*

The EML draft version 7 package [2] includes a subdirectory *samples/VIP* containing examples of Virginia 2010 VIP [7] files and an XSLT transform that includes parameters to control the generation of EML 150 and EML 505 street segment data, as well as automatically producing the EML 110 Election Event, 230 Candidate List, and 505 files.

1 Annex E – Use of EML 330 and 470 for ballot tracking

2 Annex E provides examples for using the EML 330 Election List and EML 470 Voter Token Log files for
 3 the purposes of ballot tracking. The MOVE Act [1] requires that an overseas voter be able to determine
 4 whether their ballot has been received by the appropriate EO, thus the EML 330 and 470 files can be used
 5 to send ballot status information between the BDS and the VRDB.



6
7 **Figure E-1 – The <BallotFormIdentifier> structure in EML 330**
8

9 The registration information for overseas voters can be exported from the VRDB into an EML 330 file and
 10 sent initially to the BDS. A series of <Voter> structures in the EML 330, shown in Figure E-1, contain
 11 information about each overseas voter in the file, and within each structure, one or more
 12 <BallotFormIdentifier> elements can be associated with the voter, one for each ballot that the voter is
 13 permitted to vote. Initially, each <BallotFormIdentifier> element will indicate that the ballot has not been

received by the local jurisdiction nor has it been voted, as shown in the EML 303 file example in Figure E-2. Note that the <VToken VTokenID> for voter “John Q. Public” was assigned the value “AK20111Gen12345678” – this will be used throughout to link the voter to his/her downloaded ballot.

```
<Voter>
  <VoterIdentification Id="12345678"> <!--this is the voter id that the system knows the voter by -->
    <VoterName>
      <nl:NameElement>John Q Public</nl:NameElement> <!--no explanation needed -->
    </VoterName>
    <ElectoralAddress>
      <al:FreeTextAddress>
        <al:AddressLine>123 Main Street, Hometown, AK 22034</al:AddressLine> <!--no explanation needed -->
      </al:FreeTextAddress>
    </ElectoralAddress>
    <VToken VTokenID="AK20111Gen12345678"> <!--This is a value assigned by the VRDB system and used to match back to -->
      <Component/><BallotIdentifier IdNumber="BallotF2Z666"/> <!--Generate this as the ballot form the voter is entitled to vote -->
    </VToken>
    <VoterId type="driverslicense">AK234-98765-1</VoterId>
    <!--no explanation needed == the types and values are based on what the jurisdiction makes available-->
    <VoterId type="pin">6789</VoterId> <!--multiple types and of voter identification can be provided -->
  </VoterIdentification>
  <VoterInformation>
    <DateOfBirth>1990-01-01</DateOfBirth> <!--no explanation needed -->
    <PreferredLanguage>en-us</PreferredLanguage> <!--no explanation needed == not all jurisdictions will have this available -->
    <Affiliation>Democrat</Affiliation> <!--no explanation needed -->
  </VoterInformation>
  <!--generate one line below for each ballot style the jurisdiction says the voter is entitled to vote
  on the initial feed, every line should be Permitted yes / Received no / Voted no
  the content of the element is the actual ballot style -->
  <BallotFormIdentifier Permitted="yes" Received="no" Voted="no">F2Z666</BallotFormIdentifier>
  <!--voter is permitted to vote this ballot style nothing has been received from the voter yet -->
</Voter>
```

Figure E-2 – Excerpt from initial EML 330 file “UOCAVA-BBD-example-EML330-date.xml”

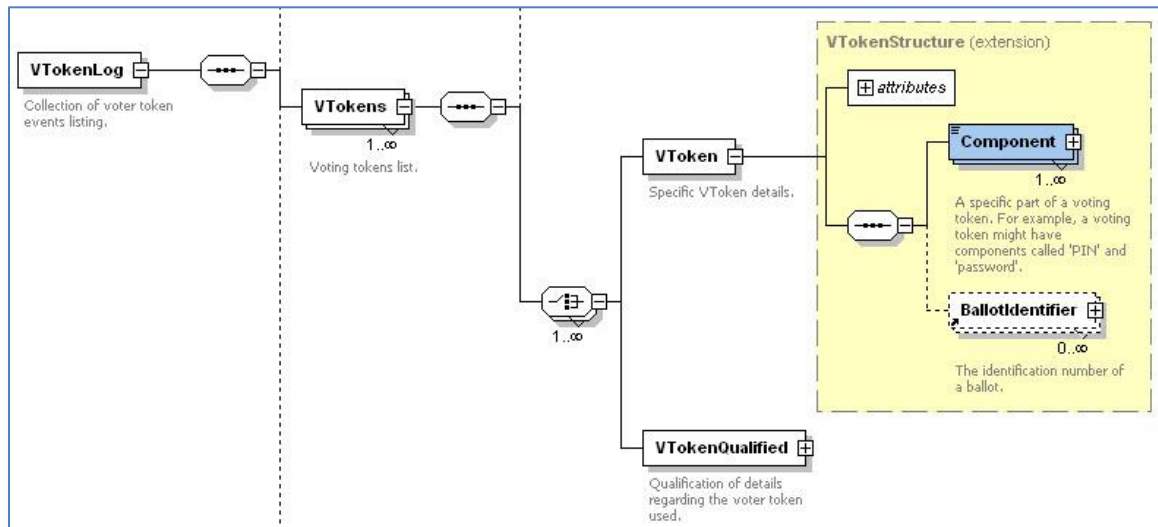


Figure E-3 – The VToken structure in EML 470

After the voter logs in to the BDS and downloads a ballot, the BDS can send a return message to the jurisdiction via an EML 470 Voter Token Log file that the voter has downloaded the ballot. The EML 470 VToken structure is shown in Figure E-3.

In the EML 470 file example shown in Figure E-4, the status is "issued" to indicate that the voter has downloaded the ballot. Upon receipt of EML 470 file, the local jurisdiction could update the VRDB with the ballot status. When the local jurisdiction subsequently receives the ballot from the overseas voter and updates the VRDB accordingly, it can then export to the EML 330 file again and send this to the VRDB as shown in the EML 330 file example in Figure E-5.

```
<VTokenLog>
  <EventIdentifier IdNumber="AK2011General"/>
  <ElectionIdentifier IdNumber="G01020304"/>
  <VTokens>
    <VotingChannel>abroad electronic</VotingChannel>
    <VToken VTokenId="AK201111Gen12345678" Status="issued">
      <!-- We want to report the status of this specific token as voted,
      unvoted, issued, submitted, received,
      rejected, resubmitted, accepted, spoiled, or exempted (those are the allowed values in the US enumeration)
      the status is then applied to the Ballots that are contained in this update local jurisdictions may use some
      of these statuses and not use others -->
      <Component/><BallotIdentifier IdNumber="BallotF2Z666"/>
      <!-- the VToken Status tells us this individual ballot was issued -->
    </VToken>
    <VToken VTokenId="AK2011Gen12345679" Status="issued"><Component/>
    <BallotIdentifier IdNumber="BallotF2Z666"/></VToken>
  </VTokens>
</VTokenLog>
```

Figure E-4 - Excerpt from EML 470 file "UOCAVA-BBD-example-EML470-date.xml"

The *<BallotFormIdentifier>* element in the updated EML 330 file has now been updated to show that the ballot has been received by the local jurisdiction. An optional *<Messages>* structure is included to show additional status that could be relayed to the voter. In the case of ballot ID F2Z666, it shows that the ballot was received on September 25, 2011 and "Rejected for Attestation Not Signed 2011-09-25." It was then presumably corrected, resubmitted, and accepted on September 26, 2011.

Upon receipt of the updated EML 330 file, the BDS can use the status and message to provide the voter the appropriate ballot status information. The method for providing status updates to the voter is left for the BDS and the jurisdiction to determine.

```

<Voter>
  <VoterIdentification Id="12345678">
    <VoterName>
      <nl:NameElement>John Q Public</nl:NameElement>
    </VoterName>
    <ElectoralAddress>
      <al:FreeTextAddress>
        <al:AddressLine>123 Main Street, Hometown, AK 22034</al:AddressLine>
      </al:FreeTextAddress>
    </ElectoralAddress>
    <VToken VTokenId="AK2011Gen12345678">
      <Component Type="PIN">Validated</Component>
      <BallotIdentifier IdNumber="BallotF2Z666"/>
    </VToken>
    <VoterId type="driverslicense">AK234-98765-1</VoterId>
    <VoterId type="pin">6789</VoterId>
  </VoterIdentification>
  <VoterInformation>
    <DateOfBirth>1990-01-01</DateOfBirth>
    <PreferredLanguage>en-us</PreferredLanguage>
    <Affiliation>Democrat</Affiliation>
  </VoterInformation>
  <BallotFormIdentifier Permitted="yes" Received="yes" Voted="yes">F2Z666</BallotFormIdentifier>
  <!--this ballot was received and it was accepted -->
  <Messages>
    <Message MessageId="F2Z666" Type="Confirm" MimeType="text/plain"
      DateTime="2011-09-26T13:13:13">F2Z666 Accepted 2011-09-26</Message>
    <Message MessageId="F2Z666" Type="Reject" MimeType="text/plain"
      DateTime="2011-09-25T09:27:01">F2Z666 Rejected for Attestation Not Signed 2011-09-25</Message>
  </Messages>
</Voter>

```

1

2

3

Figure E-5 - Excerpt from updated EML 330 file “UOCAVA-BBD-example-EML330u-date.xml”

1 Annex F - Example of using the SEAL digital signature structure

2 An EML file can be digitally signed, with information about the digital signature, including algorithm,
 3 canonicalization method, and the digital signature value placed within the file using the EML SEAL
 4 structure, which is based on the W3C XML Signature Syntax and Processing [9]. The “UOCAVA-BBD-
 5 example-EML470WithSeal-date.xml” example file is digitally signed and includes the SEAL structure,
 6 shown in Figure F-1, whereas the other example files include a comment indicating where the SEAL
 7 structure would be placed (in the header of the file).

```

<Seal>
<!--This is a sample of a seal ; it provides a digital signature that allows viewers to verify that the content is unchanged
from when it was published -->
  <ds:Signature>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="">
        <!--leaving the URI attribute empty causes the entire message tree to be included, except for exclusions from
the subsequent xpath element -->
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116"><ds:XPath>not(EML::SEAL)</ds:XPath>
          </ds:Transform><!--everything except this seal will be used to generate a digest -->
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>fUVZ96IZAOgQcryJBzEGsRVqMzs=</ds:DigestValue>
        <!--this is the digest value for the content of this message, excluding the xpath excluded parts -->
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="SignatureValue">
BhUHx1yaMfAVJLmw4QUG0FpRmZH30Amej8hy31dL4hxUMlzw/B9kAzXe+QBgi5VtPKTr/rM99x+ze1VBGrBclPceFgtz/FYgtgsPiKs69
hVL82QzF/1pfcA3DvppeczNONnqRh2af357HVR0AdgfxlmVWvFkQFWI2avyqAxWK+I=</ds:SignatureValue>
    <!-- this is the digital signature for the above digest, if the digital signature is valid and the digest is valid then the content is valid-->
    <ds:KeyInfo>
      <ds:KeyName>TheNameByWhichThePublicKeyForTheSigningEntityCanBeRetrievedFromTheCertificateAuthority</ds:KeyName>
    </ds:KeyInfo>
  </ds:Signature>
</Seal>

```

8
 9 **Figure F-1 –The EML SEAL digital signature structure, excerpted from UOCAVA-BBD-**
 10 **example-EML470WithSeal-date.xml**

11
 12 Note that this is being provided for illustrative purposes and not as a model for exact usage. Formal
 13 guidance on using the SEAL structure and digital signatures is beyond the scope of this document, however
 14 guidelines can be noted for digital signatures to verify properly. In particular, attention will have to be paid
 15 to the canonicalization method used (e.g., consistently using a method such as Canonical XML 1.1² or later
 16 version) and the algorithms employed (adherence to FIPS 186-3³), as well as to the scope of how the file is
 17 signed, with a simple recommendation being that all contents of the file be signed as opposed to some
 18 subset. The SEAL structure in the “UOCAVA-BBD-example-EML470WithSeal-date.xml” example file
 19 contains the actual digital signature of the file, which was generated on the entire file (except for the SEAL
 20 structure).

² See <http://www.w3.org/TR/xml-c14n11/#XMLCanonicalization>.

³ See http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.