IEEE P1622™/D4
Draft Standard for Electronic Distribution of Blank Ballots for Voting Systems

Sponsor

Voting Equipment Electronic Data Interchange Committee
of the
IEEE Computer Society

Approved <XX MONTH 20XX>

IEEE-SA Standards Board

Abstract: This standard specifies electronic data interchange formats for blank ballot distribution, primarily to assist in satisfying 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. The P1622 Voting Equipment Electronic Data Interchange Committee produces this standard.

Keywords: absentee voting, blank ballot distribution, elections, EML, FVAP, military voters, MOVE Act, overseas voters, UOCAVA, VIP, voting systems, vote-by-mail.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

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

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, an 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.

Introduction

This introduction is not part of IEEE P1622/D4, Draft Standard for Electronic Distribution of Blank Ballots for Voting Systems.

The current practice of distributing blank paper ballots to UOCAVA voters using conventional postal mail can involve considerable delays, imperiling their timely return. To help overcome these barriers, Section 584 of the Military and Overseas Voter Empowerment (MOVE) Act requires states to provide for UOCAVA voters at least one electronic method for requesting and receiving voter registration applications, absentee ballot requests and related election information. Also, Section 585 requires states to provide an electronic transmission method for the delivery of blank ballots. Thus, this standard is intended to assist state and local election officials in making available electronic blank ballots to UOCAVA voters in a manner directly akin to absentee voting. Specifically, this standard provides XML-based data structures to be used for export of election information necessary to construct electronic blank ballots.

Notice to users

Laws and regulations

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

Copyrights

Updating of IEEE documents

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

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

Errata

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

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

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

Participants

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

Arthur M. Keller, *Chair*
Stephen Berger, *Vice-Chair*
John P. Wack, *Vice Chair*
Carmelo Montanez-Rivera, *Secretary*

John Borras	Kurt Hyde	Paul Miller
Duncan Buell	James Long	Ian Piper
Rita Eaton	Neal McBurnett	David Webber
Susan Eustis	John McCarthy	Peter Zelechoski

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

(to be supplied by IEEE)

Balloter1	Balloter4	Balloter7
Balloter2	Balloter5	Balloter8
Balloter3	Balloter6	Balloter9

When the IEEE-SA Standards Board approved this standard on <XX MONTH 20XX>, it had the following membership:

(to be supplied by IEEE)

<Name>, *Chair*
<Name>, *Vice Chair*
<Name>, *Past President*
<Name>, *Secretary*

SBMember1	SBMember4	SBMember7
SBMember2	SBMember5	SBMember8
SBMember3	SBMember6	SBMember9

*Member Emeritus

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

<Name>, *NRC Representative*
<Name>, *DOE Representative*
<Name>, *NIST Representative*

<Name>
IEEE Standards Program Manager, Document Development

<Name>
IEEE Standards Program Manager, Technical Program Development

Contents

Draft 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.

1. Overview

1.1 Scope

This standard specifies XML-based electronic data interchange formats for blank ballot distribution, primarily to satisfy the needs of the UOCAVA (Uniform and Overseas Citizens Assistance in Voting Act) and MOVE (Military and Overseas Voter Empowerment) Acts. Subsequent standards may 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.

1.2 Purpose

This standard defines common data interchange formats to allow export of blank ballots from voting systems, primarily to facilitate the casting of ballots by military and overseas voters.

1.3 Additional Rationale

The XML-based electronic data interchange formats are to allow export of information from voting systems to facilitate the construction of electronic blank ballots for use with ballot delivery systems (BDSs) such that ballots can be downloaded from a BDS and then printed and returned and processed in a manner directly akin to absentee voting. The XML schemas and elements described therein are included as part of OASIS Election Markup Language (EML) v7.0.

Additionally, 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 (UOCAVA) [B2], [B3] and the Military and Overseas Voter Empowerment (MOVE) Act [B1], i.e., to assist UOCAVA voters in participating fully in U.S. elections. It may also be useful for other applications, such as permitting consistent export of information between voter registration database systems (VRDBs) and BDSs.[1]

1.4 Document structure

The main body of this standard serves primarily to explain the background and concept for this standard and to show major steps in using the files referenced by this standard. The annexes of this standard deal with specific EML schemas and files and requirements as to their usage.

2. 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. Key words for use in RFCs to Indicate Requirement Levels, Internet Engineering Task Force RFC 2119, March 1997.[2]

OASIS Election Markup Language (EML) Version 7.0.[3]

P1622 IEEE UOCAVA BBD Example Files.[4]

Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation November 26, 2008.[5]

XML Signature Syntax and Processing (Second Edition), W3C Recommendation June 10, 2008.[6]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary: Glossary of Terms & Definitions* should be consulted for terms not defined in this clause.[7]

blank ballot: The official presentation of all of the contests to be decided in a particular election. (From Voluntary Voting System Guidelines, Version 1.0, [B5].)

NOTE—The ballot presentation can be a collection of one or more pieces of paper or an electronic representation, such as a PDF document or JPEG image.

ballot configuration: A set of contests, including vote variation information, in which voters of a particular group (e.g., political party and/or election district) are entitled to vote.

ballot rotation: The process of varying the order of the contest choices within a given contest.

[1] Future P1622 standards may address VRDB export and other aspects of election data.
[2] This document is available from the IETF Web site http://www.ietf.org/rfc/rfc2119.txt.
[3] This document is available from the OASIS Web site http://docs.oasis-open.org/election/eml/v7.0/eml-v7.0.html.
[4] The example files for this standard are available from the IEEE P1622 Web site http://grouper.ieee.org/groups/1622/p1622documents.html.
[5] This document is available from the W3C Web site http://www.w3.org/TR/xml/.
[6] This document is available from the W3C Web site http://www.w3.org/TR/xmldsig-core/.
[7] *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at http://shop.ieee.org/.

contest: (A) A single decision being put before the voters (e.g., the selection of candidates to fill a particular public office or the approval or disapproval of a constitutional amendment). **(B)** A subdivision of a ballot pertaining to a single decision being put before the voters.

election district: Contiguous geographic area represented by a public official who is elected by voters residing within the district boundaries. The district may cover an entire state or political subdivision, may be a portion of the state or political subdivision, or may include portions of more than one political subdivision. (From Voluntary Voting System Guidelines, Version 1.0, [B5].) *See also:* **precinct**; **split precinct**.

electronic blank ballot: *See:* **blank ballot**.

generic ballot style: A ballot configuration that includes the ordering information regarding how the contests appear but does not include U.S. State-required formatting details such as specific fonts or sizes or other layout.

overseas voter: A U.S. citizen living temporarily or permanently outside of the U.S. who is eligible to vote in their place of residence in the U.S.

precinct: An election administration division corresponding to a contiguous geographic area that is the basis for determining which contests and issues the voters legally residing in that area are eligible to vote on. (From Voluntary Voting System Guidelines, Version 1.0, [B5].) *See also:* **election district**; **split precinct**.

schema: An XML file containing definitions of data elements and attributes with rules for usage.

split precinct: A precinct that contains an election district subdivision requiring that a portion of the voters assigned to the precinct be given a ballot configuration that is different from the remainder of the voters assigned to the precinct. (Adapted from Voluntary Voting System Guidelines, Version 1.0, [B5].)

NOTE—For example, a water district or school board district within a precinct could include ballot items specific to the district but not to the precinct at large.

street segment data: The portion of a street between two consecutive cross streets that can be assigned to a voting precinct.

UOCAVA voter: An overseas voter or an active duty member of the U.S. military both within and outside of the U.S. including any accompanying spouse and family members who are eligible to vote in their place of residence in the U.S. *See also:* **overseas voter**.

voting variation: A voting style, option, or feature such as in-person voting, absentee voting, provisional / challenged ballots, review-required ballots, closed primaries, open primaries, write-ins, ballot rotation, straight party voting, cross-party endorsement, split precincts, N-of-M voting, cumulative voting, approval voting, range voting, or ranked order voting.

3.2 Acronyms and abbreviations

BDS	ballot delivery system
EML	election markup language
EMS	election management system
EO	election official
FIPS	Federal Information Processing Standard

FVAP	Federal Voting Assistance Program[8]
FWAB	federal write-in absentee ballot
MOVE	Military and Overseas Voter Empowerment Act
OASIS	Organization for the Advancement of Structured Information Standards[9]
UML	unified modeling language
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act
VIP	Voting Information Project
VRDB	voter registration database
XML	extensible markup language

4. Document Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in “Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119.” In particular, the key word "SHALL" means that the definition is an absolute requirement of this standard and the key word "SHOULD" means that there may exist valid reasons in particular circumstances to ignore a particular item but the full implications must be understood and carefully weighed before choosing a different course. When the usage of any of these key words in this standard is to be interpreted as described in RFC 2119, the key word is placed in all capitals, i.e., “SHALL.”

This standard references EML version 7 XML schemas and files. Conformant applications SHALL observe all rules of XML usage and SHALL produce only XML that is well-formed[10] and valid according to EML version 7 base schemas. Conformant applications SHALL use EML version 7 schemas in the manner described in this standard. Use of future versions of EML is permitted to claim conformance to this standard, if the resulting EML conforms to the data specification of this standard.

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 Charitable Trusts’ Voting Information Project [B4] (VIP), which assists voters in finding their voting locations and showing the contests/issues on their ballot. Conformant implementations of this standard SHALL use the data elements and structures of the EML 505, or they SHALL use the identical data elements and structures as found in the schemas that collectively constitute the EML 505, these being the EML 110, 230, and 410 (see Annex E for information regarding the other base EML schemas). Additionally, conformant implementations SHALL use the EML 330 to exchange information about which voters are entitled to which ballots and ballot status information for the given election event, and conformant implementations SHALL use the EML 470 to return information from the BDS to the VRDB to facilitate the ballot status tracking requirements of the MOVE Act [B1] (see Annex F for details on the use of the EML 330 and 470).

Other normative language and requirements in this standard are contained primarily in the annexes of this standard for purposes of organization and brevity. The main body of this standard serves primarily to explain the background and concept for this standard and show major steps in using the files referenced by this standard.

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

[8] See the information at the following Internet location: http://www.fvap.gov.
[9] See the information at the following Internet location: http://www.oasis-open.org.
[10] See Extensible Markup Language (XML) 1.0 (Fifth Edition) Section 2.1 at the W3C Web site http://www.w3.org/TR/REC-xml/#sec-well-formed.

voting. Specifically, it provides XML schemas and examples in EML version 7 for the purposes of exporting from VRDBs and Election Management Systems (EMS), in a common XML format, the election district information and ballot definition information needed to facilitate automated construction of electronic blank ballots. It also provides the opportunity for UOCAVA voters to track the status of their ballot, as required in the MOVE Act [B1]. This standard does not make provisions for the electronic return of ballots, nor for verifying a voter's entitlement to vote.

An EML 505 file can be built to serve two basic purposes: (a) for use in indexing from UOCAVA voters' election district 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 (a) election district and (b) election information to an EML 505 and including the appropriate linkage to the blank ballots (e.g., a collection of PDF blank ballot files).

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

During voting:

c) 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 election district 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 election district information stored within an EML 505 file and then to the generic ballot style 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).

Additionally, the MOVE Act [B1] requires that a UOCAVA voter be able to determine whether his or her 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.

6. Actors, stakeholders

There are two primary actors for this standard[11]:

— The UOCAVA voter, who requests and retrieves a blank ballot.

— The EO (state/local or FVAP), who prepares ballot information beforehand and receives the returned ballot from the UOCAVA voter.

Primary stakeholders for this standard include:

[11] There could also be intermediaries intentionally interposed between the voter and the EO, e.g., FVAP, that facilitate blank ballot delivery.

- EOs in U.S. States or territories.
- The Federal Voting Assistance Program (FVAP) in implementing the UOCAVA [B2], [B3] and MOVE Act [B1].
- UOCAVA voters including military and citizens stationed or residing abroad.

7. Assumptions, pre-conditions

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

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

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

d) Exports from VRDBs of voter registration data and election district data for UOCAVA voters for the purposes of identifying each voter and presenting the correct ballot.
e) Exports from EMSs (for both election district data and ballot description data) for construction of the ballot.
f) If electronic blank ballots are to be created before the election and stored for later retrieval by UOCAVA voters, then preparation of the electronic blank ballots and storage in BDSs.
g) 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.

8. Main scenario

This clause 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 UOCAVA 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 UOCAVA voter and then in performing subsequent status updates and tabulations. The UOCAVA voter is engaged in requesting a ballot, marking/printing the ballot, and mailing it to the voter's respective election district (or other designated postal site).

The steps below outline the activities of the EO:

a) The EO exports UOCAVA voter registration information from the VRDB into an EML 330 Election List file, including items such as voter name, registered address, and details about party affiliation and ballot type. The EO sends updated EML 330 file to the BDS for use in establishing its database of UOCAVA voters permitted to connect to the BDS to download ballots. Periodically during the election, EOs may refresh the BDS with additional EML 330 exports as UOCAVA voters are added, modified, or deleted from the VRDB.
b) The EO exports election data from the VRDB 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 UOCAVA voters are eligible to participate and the corresponding ballots. The election data includes:
    1) Information necessary for locating the voter's precinct, including election district information, precinct information, or street segment data.

2) Contest, candidate, and issues information for each ballot.

3) Information necessary to create a generic ballot style (if ballots are being constructed dynamically to display to the voter).

c) If the BDS will be retrieving pre-constructed electronic blank ballots (and not building them dynamically), the EML 505 file would be populated with indices to externally-located electronic blank ballots as opposed to the information in item 3, above.

d) 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.

e) The EO receives printed ballots as voters return them via postal mail. The EO updates the VRDB with status regarding the received ballots, e.g., ballot accepted, rejected (the processing of these ballots is comparable to that of processing absentee ballots).

f) 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 UOCAVA voters with the status of their received ballots.

The steps below outline the activities of the UOCAVA voter:

g) A UOCAVA voter uses a BDS to enter information about themselves, e.g., their name, address, etc. The BDS then uses the information to identify the voter, the voter's party affiliation (as necessary), and the voter's election district, and then whether the voter is eligible to vote in any elections taking place in the voter's election district.

h) If the voter is eligible to vote in the election, the voter downloads the ballot.

i) If electronic ballot marking is available, the voter may make ballot selections among the races and issues and then print the marked paper ballot. If electronic ballot marking is not used, the voter will print the ballot and mark ballot selections on the printed ballot by hand.

j) The voter then places the printed ballot in an envelope. Depending upon a state's requirements, the voter may include a signed declaration form attesting that the voter is eligible to vote in the election. For privacy, the printed ballot may be placed in an inner envelope, and the inner envelope is placed along with the signed declaration form in an outer envelope.

k) The voter mails the envelope to the EO or to some other designated postal site.

l) According to the MOVE Act [B1], the voter can check on the status of his or her received ballot, e.g., receive an e-mail update from the BDS regarding whether the voter's ballot has been received.

Figure 1 models these steps from the perspectives of the UOCAVA 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.

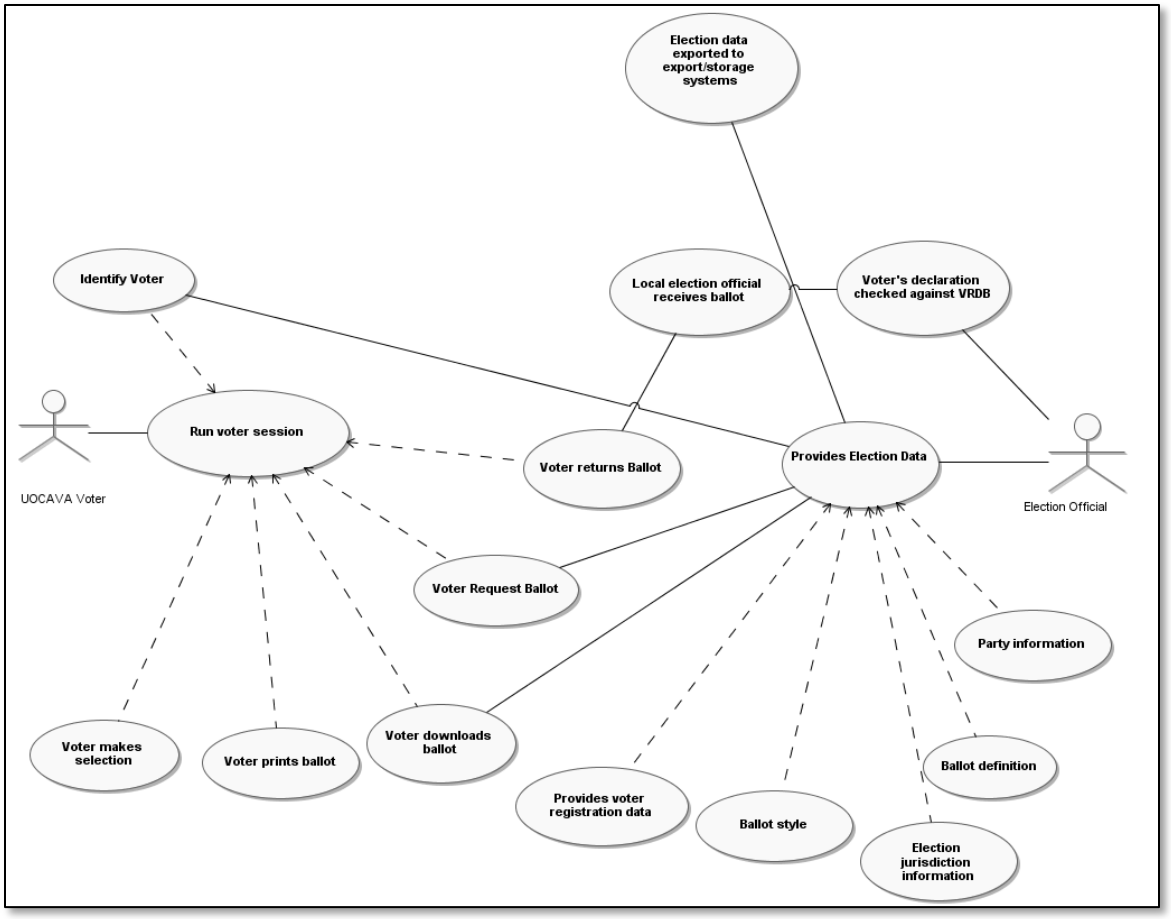

Figure 1: Blank ballot distribution model

9. 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 is to appear on the screen or how the ballot is to appear in print.

e) Ballot return data such as the address where ballots are to be returned or drop shipment data.

f) Declaration form that the voter can use to attest they are eligible to vote in the election.

10. Security considerations

There are a number of security considerations associated directly or tangentially with this standard that are beyond the scope of this standard but at the same time important to discuss. One direct consideration is that the EML files discussed in this standard will contain election information whose integrity, authenticity, and proof of origin (non-repudiation) is critical to the successful conduct of the election; errors in the information as a result of malicious or otherwise intent could selectively disenfranchise voters and prevent them from participating in elections, or worse. Accordingly, implementations SHOULD digitally sign EML files using stand-alone systems, i.e., those never connected to the Internet, when creating them. They SHOULD also validate those signatures using stand-alone systems after receiving them. Conformant implementations, when digitally signing EML files, SHALL use the SEAL element as described in Annex G, which provides for a digital signature that can be checked for content integrity, authenticity, and proof of origin. For digital signature hardware and software modules, conformance to FIPS 140-2 [B6] may be required in U.S. Government procurements.

Protecting the authenticity and integrity of EML files with the SEAL structure is only one step in providing the requisite security required for successful construction and delivery of electronic blank ballots. EML files will be used on BDSs and other systems that will be connected to the Internet and therefore at risk to a variety of different threats and attacks, some of which are difficult to defend against such as denial-of-service attacks and some which involve aspects of social engineering such as phishing attacks in which a fake web site may masquerade as a legitimate entity. Using the SEAL structure protects the integrity of the EML files in case of Internet-borne attacks, but if system or application security is penetrated, the overall integrity of the system and its data can no longer be trusted. Application and system security will be critically important to protect; conformance to security standards including FIPS 200 [B7], the requirements in NIST Special Publication 800-53 [B8], and Common Criteria Protection Profile BSI-CC-PP-0037 [B9], may be required in U.S. Government procurements.

For additional background information, NISTIR 7551, A Threat Analysis on UOCAVA Voting Systems [B10], and NISTIR 7770, Security Considerations for Remote Electronic UOCAVA Voting [B11], can be consulted. NISTIR 7551 documents the threats to UOCAVA voting systems using electronic technologies for all aspects of overseas and military voting. NISTIR 7551 considers the use of postal mail, telephone, fax, electronic mail, and web servers to facilitate transmission of voter registration materials, blank ballots, and cast ballots. NISTIR 7770 identifies and defines desirable security properties of remote electronic voting systems and major threats faced by these systems that could violate those security properties. It also discusses the current technologies that could be used to mitigate some of those threats and open issues that still need to be addressed.

11. Additional notes

11.1 Applicability to online ballot return

Online (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 as well as additional data.

11.2 Overseas printing issues

Overseas military and citizens, if printing downloaded ballots, can require different paper sizes (e.g., A4) and printer formats than those commonly used in the U.S. (e.g., U.S. Letter). This standard does not deal with paper sizes and printer formats, however applications involving use of this standard will need to anticipate these needs and program accordingly. Online ballots SHOULD be supplied online in both U.S. Letter optimized and A4 optimized sizes.

11.3 Return address for ballots usage in EML

UOCAVA voters, if using a BDS to download a ballot to subsequently print and return by postal mail, SHALL be provided the return address. The EML 110 file's <PollingPlace channel="postal"> structure[12] SHOULD be used, as provided in the example below:

```
<PollingPlace Channel="postal">
  <PostalLocation IdNumber="UOCAVABallotReturn">
    <al:FreeTextAddress>
      <al:AddressLine>PO Box 1234, Municipality, MyState 98765-1234
      </al:AddressLine>
    </al:FreeTextAddress>
  </PostalLocation>
  <TimeAvailable>
    <Start>2006-11-27T00:00:01</Start>
    <End>2006-12-10T20:00:00</End>
  </TimeAvailable>
</PollingPlace>
```

[12] This usage of the <PollingPlace> structure overrides any usage of the <ManagingAuthority> structure's <AuthorityAddress> element.

Annex A

(informative)

Bibliography

[B1] Military and Overseas Voter Empowerment (MOVE) Act, 2010, http://ballotpedia.org/wiki/index.php/Military_and_Overseas_Voter_Empowerment_(MOVE)_Act.

[B2] Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) as amended by the MOVE Act, 2010, http://www.fvap.gov/resources/media/uocavalaw.pdf.

[B3] Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes, U.S. Election Assistance Commission, April 6, 2011, http://www.eac.gov/assets/1/Documents/UOCAVA_Registration_and_Voting_Processes.pdf.

[B4] Voting Information Project (VIP), PEW Center on the States, http://www.pewcenteronthestates.org/uploadedFiles/Voting_Information_Project_brief.pdf.

[B5] Voluntary Voting System Guidelines, Version 1.0, http://www.eac.gov/testing_and_certification/2005_vvsg.aspx.

[B6] Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[B7] Federal Information Processing Standard 200, Minimum Security Requirements for Federal Information and Information Systems, National Institute of Standards and Technology, March 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[B8] Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, National Institute of Standards and Technology, May 2010, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[B9] Common Criteria Protection Profile BSI-CC-PP-0037, Basic set of security requirements for Online Voting Products, M. Volkamer and R. Vogt, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0037b_engl_pdf.pdf?__blob=publicationFile.

[B10] NISTIR 7551, A Threat Analysis on UOCAVA Voting Systems, National Institute of Standards and Technology Interagency Report, December 2008, http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf.

[B11] NISTIR 7770, Security Considerations for Remote Electronic UOCAVA Voting, National Institute of Standards and Technology Interagency Report, February 2011, http://www.nist.gov/itl/vote/upload/NISTIR-7770-feb2011-2.pdf.

[B12] Special Publication 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, National Institute of Standards and Technology, September 2011, http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.

[B13] Federal Information Processing Standard 186-3, Digital Signature Standard, National Institute of Standards and Technology, June 2009, http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

Annex B

(informative)

Example files

The Election Markup Language (EML) version 7 example files that correspond to the figures and descriptions in this standard are available as a "zip" archive file using the URL below:

http://grouper.ieee.org/groups/1622/examples/EML-v7-samples.zip

To validate properly, place the zip file in a directory containing the EML version 7 distribution, e.g., /EMLv7, and then expand it. This will create a directory structure of

/EMLv7/EML-v7-samples/UOCAVA

The following files are included in the EML-v7-samples.zip file:

- UOCAVA-BBD-example-EML330-*yyyymmdd*.xml
- UOCAVA-BBD-example-EML330u-*yyyymmdd*.xml
- UOCAVA-BBD-example-EML410-*yyyymmdd*.xml
- UOCAVA-BBD-example-EML470-*yyyymmdd*.xml
- UOCAVA-BBD-example-EML505-*yyyymmdd*.xml (shares the same contest data as in UOCAVA-BBD-example-EML410-*yyyymmdd*.xml)
- UOCAVA-BBD-example-ballot-F2Z666-*yyyymmdd*.pdf (can be generated from EML 410 or 505 files)
- UOCAVA-BBD-example-ballot-F3Y111-*yyyymmdd*.pdf (can be generated from EML 410 or 505 files)

where *yyyymmdd* is year, month, day, such that "20111201" is December 1, 2011.

The zip file also includes a subdirectory EML-v7-samples/VIP containing examples of the Pew Charitable Trusts' Voting Information Project (VIP) [B4] 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.

Annex C

(normative)

The EML 505 schema and file

The Election Markup Language (EML) 505 schema was designed for this standard and for general use in creating electronic blank ballots for UOCAVA voters. The 505 schema is composed of XML structures found also in other base EML schemas, however it has been optimized to make it convenient to use with the PEW Foundation's Voter Information Project [B4] (VIP), which assists voters in finding their voting locations and showing the contests/issues on their ballot.

Conformant implementations of this standard SHALL use the data elements and structures of the EML 505, or they SHALL use the identical data elements and structures as found in the schemas that collectively constitute the EML 505, these being the EML 110, 230, and 410 (see Annex E for information regarding the other base EML schemas).

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

a) A structure that describes various election authority details
b) A series of linked structures that describe information on
    1) Voting location information (localities, locality boundaries, districts, polling locations).
    2) Information on the elections in each precinct.
    3) Contests and propositions in corresponding elections including vote variation information and the order in which the contests appear on the ballot, and candidates in the contests.

The election information and linked structures are populated from exports from the voter registration database (VRDB) and election management system (EMS). The contest information links to a ballot ID, which can be used by a ballot delivery system (BDS) for either of the following:

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

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

Annex D discusses using the EML 505 file to point to electronic blank ballots located externally.

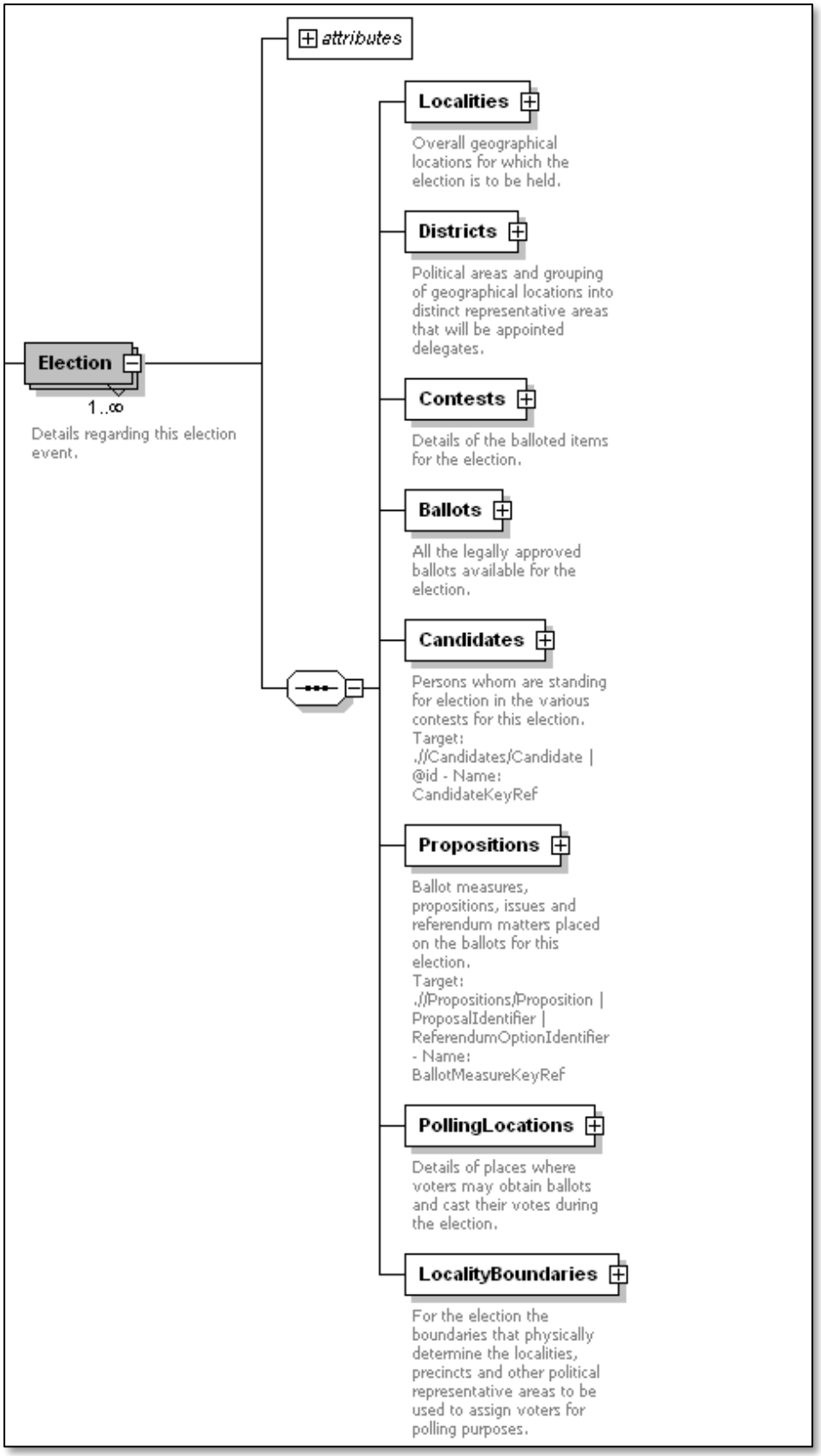

Figure C.1—EML 505 main structures

Annex D

(normative)

The EML 505 using pre-constructed electronic blank ballots

From Annex C, 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 using an associated identifier, or
    2) By pointing to a URL where a blank ballot file ballot can be retrieved.

This annex includes requirements and example usage for pointing to pre-constructed electronic blank ballots with an EML 505 file. Figure D.1 below shows the portion of the EML 505 schema that identifies a ballot and Figure D.2 is an XML file instance of this portion of the schema, using example data.

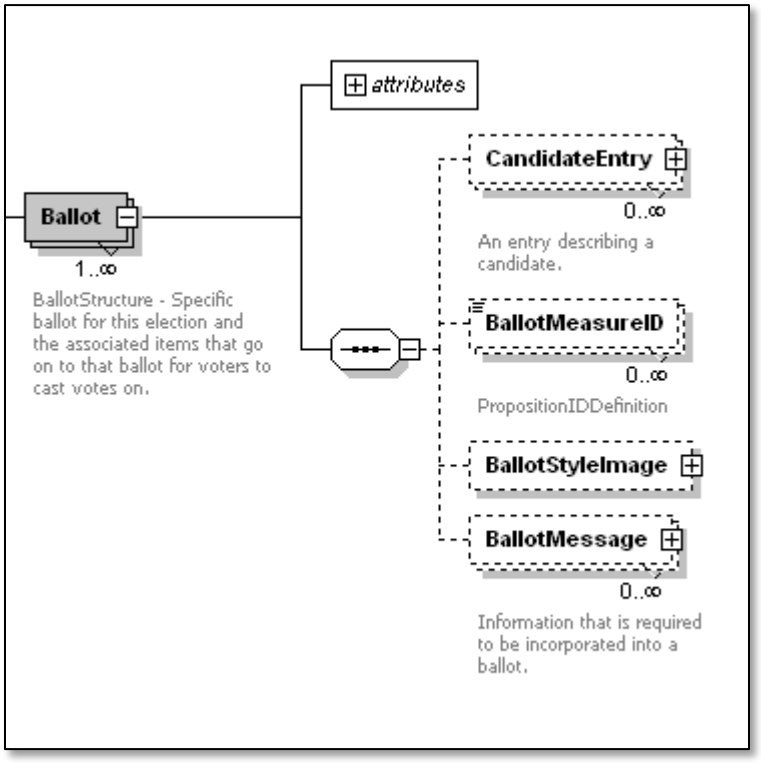

Figure D.1—EML 505 schema ballot structure

D.1 Using an identifier to index to a blank ballot file

Conformant implementations SHALL use the <*Ballot id*> field to identify a corresponding electronic blank ballot file stored externally. In Figure D.2, the identifier is "F3Y111," used to index to the corresponding electronic blank ballot located in, e.g., a data store of PDF files.

```
- <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
        MimeType="application/pdf">http://grouper.ieee.org/groups/1622/examples/UOCAVA
        -BBD-example-ballot-F3Y111-20110607.pdf</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 D.2—Excerpt from EML 505 file "UOCAVA-BBD-example-EML505-*yyyymmdd*.xml"

D.2 Using a URL to index to a blank ballot file

Figure D.2 also shows the <*BallotStyleImage*><*URL*> element. Its value is a pointer to a blank ballot file located at the URL http://grouper.ieee.org/groups/1622/examples/UOCAVA-BBD-example-ballot-F3Y111-20110607.pdf. Conformant implementations, if referencing a blank ballot file located on a web site, SHALL use the <*BallotStyleImage*><*URL*> element to reference the blank ballot file[13].

[13] While the <URL> element permits additional fields for including a hash code of the file referenced by the URL, the required method for including a hash code uses the EML SEAL element, described in Annex G.

Annex E

(informative)

Other base EML schemas

From Annex C, other base EML schemas that provide the same data structures as found in the EML 505 schema could be employed instead or in addition to those of the EML 505. The other base EML schemas that contain the same structures as in the EML 505 schema are:

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

This standard includes an example EML 410 file (UOCAVA-BBD-example-EML410-*yyyymmdd*.xml) whose contest structure information was used also in the example EML 505 file (UOCAVA-BBD-example-EML505-*yyyymmdd*.xml). The EML 410 and 505 examples contain ballot information to build two example ballots (UOCAVA-BBD-example-ballot-F2Z666-*yyyymmdd*.pdf, shown in Figure E.1 and UOCAVA-BBD-example-ballot-F3Y111- *yyyymmdd*.pdf). The contest structure of the EML 410 is shown in Figure E.2.

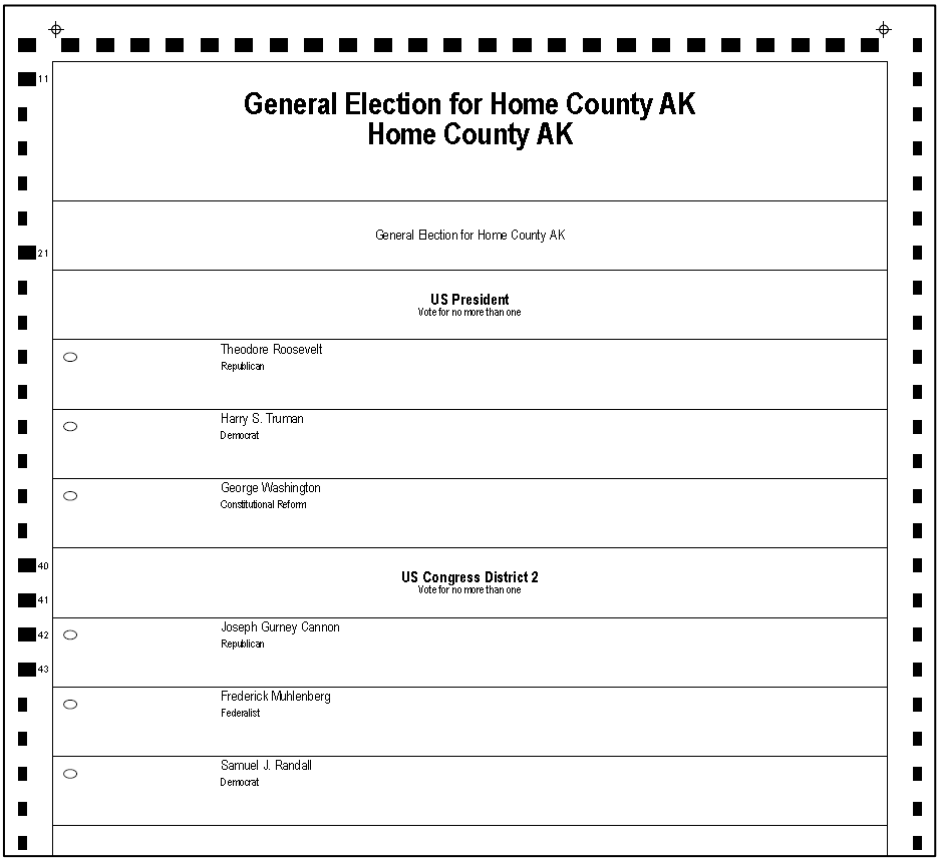

Figure E.1—Example ballot built from "UOCAVA-BBD-example-EML410-yyyymmdd.xml" (or "–EML505-yyyymmdd.xml")

From Annex B, the EML version 7 package includes a subdirectory *samples/VIP* containing examples of Virginia 2010 VIP [B4] 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.

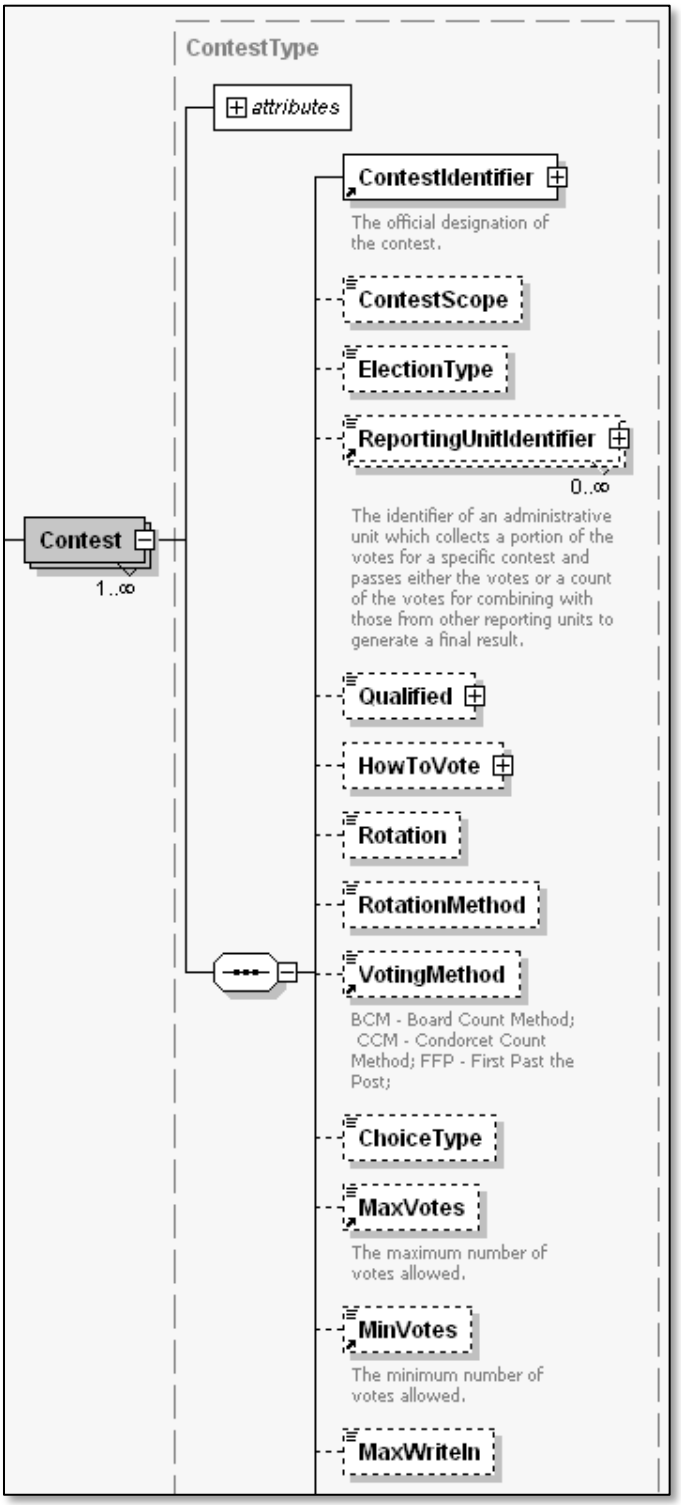

Figure E.2—The EML 410 contest structure

Annex F

(normative)

The EML 330 and 470 for ballot tracking

This annex provides requirements and examples for using the EML 330 Election List and EML 470 Voter Token Log files for the purposes of ballot tracking. The Military and Overseas Voter Empowerment Act (MOVE) Act [B1] requires that a UOCAVA voter be able to determine whether their ballot has been received by the appropriate election official (EO), thus the EML 330 and 470 files SHALL be used to send ballot status information between the BDS and the VRDB.

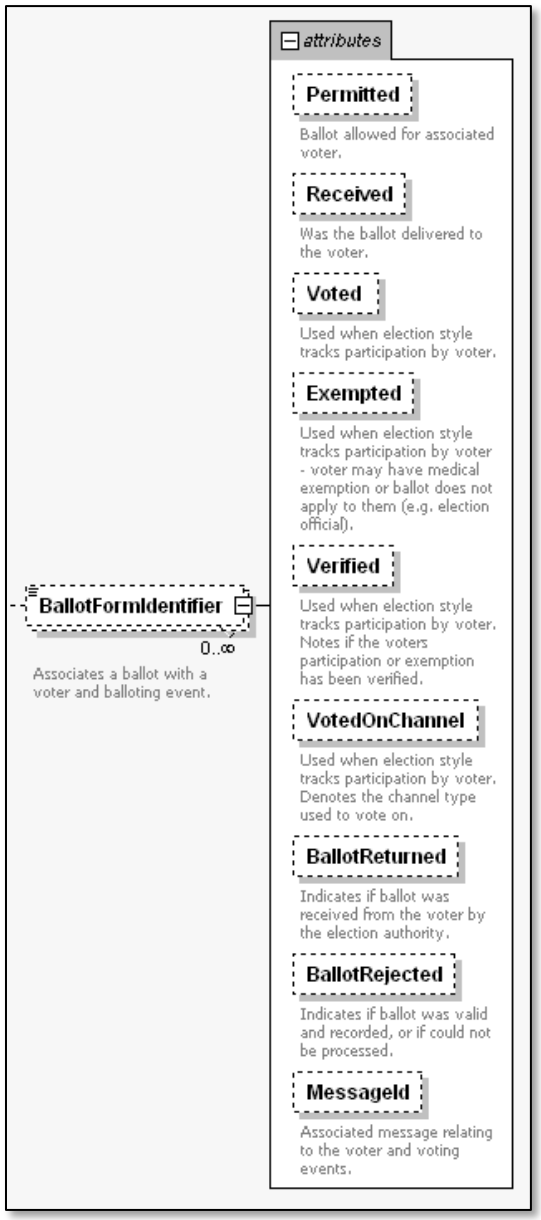

Figure F.1—The <*BallotFormIdentifier*> structure in EML 330

The registration information for UOCAVA voters can be exported from the VRDB into an EML 330 file and sent initially to the BDS. A series of <*Voter*> structures in the EML 330 file contain information about each UOCAVA voter in the file, and within each structure, one or more <*BallotFormIdentifier*> elements, shown in Figure F.1, are associated with the voter, one for each ballot that the voter is 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 F.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 the status of his/her downloaded ballot.[14]

```
- <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="AK2011Gen12345678">
        <!-- 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 F.2—Excerpt from initial EML 330 file "UOCAVA-BBD-example-EML330-*yyyymmdd*.xml"

After the voter logs in to the BDS and downloads a ballot, the BDS SHALL 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 F.3.

[14] Note that the VToken does not include a pointer to the voter's ballot, only to a status of its use, thus the privacy of the voter's ballot selections is preserved.

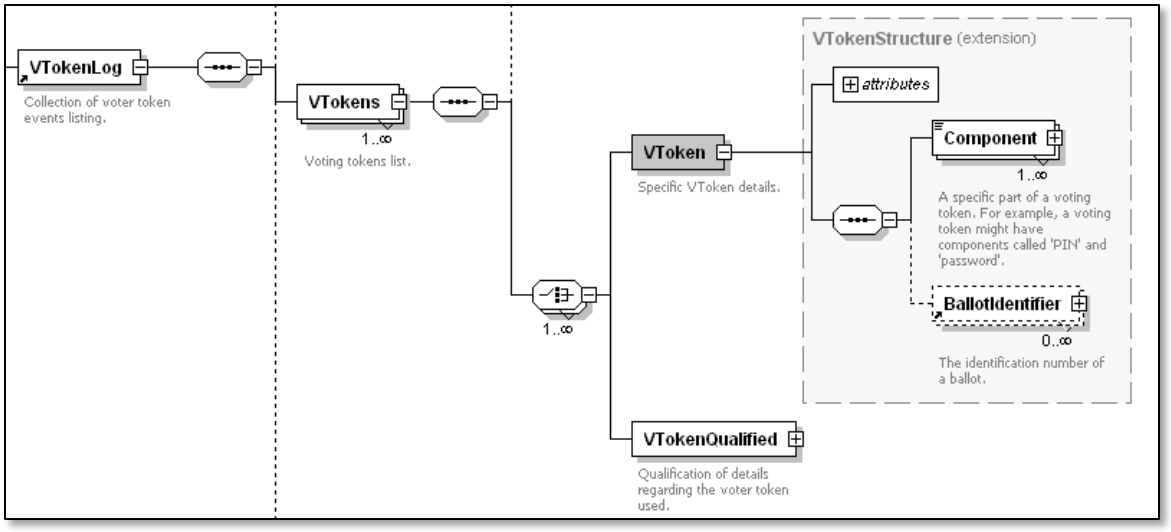

Figure F.3—The VToken structure in EML 470

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

```
- <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 F.4—Excerpt from EML470 file "UOCAVA-BBD-example-EML470-*yyyymmdd*.xml"

The <*BallotFormIdentifier*> element shown in Figure F.5 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 to 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.

```
- <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>
```

Figure F.5—Excerpt from updated EML 330 file "UOCAVA-BBD-example-EML330u-*yyyymmdd*.xml"

Upon receipt of the updated EML 330 file, the BDS SHALL 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.

Annex G

(normative)

The SEAL digital signature element

To establish the provenance of an EML file, it SHOULD be signed. EML uses W3C's XML Signature Syntax and Processing for signatures. The Signature element is placed inside the EML SEAL element, within the EML header. When signing EML files, applications conformant to this standard SHALL use the W3C XML Signature element within the SEAL element.

Figure G.1 shows part of the SEAL element in the UOCAVA-BBD-example-EML505-yyyymmdd.xml example 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/2001/04/xmldsig-more#rsa-sha256" />
      - <ds:Reference>
          <!-- leaving out the URI attribute causes the entire message tree to be included, except for exclusions from
          the subsequent transform   -->
        - <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <ds:DigestValue>jXadqiDS+ADYQWYLtE78PgE97TLxd0vhTIls3J8CvYA=</ds:DigestValue>
          <!-- this is the digest value for the content of this message, excluding the transform-excluded parts   -->
        </ds:Reference>
      - <ds:Reference Type="http://www.w3.org/2000/09/xmldsig#Manifest" URI="#manifest-20110707112708271-61">
        - <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <ds:DigestValue>6dcNQ5QADRgG8yO2bJCk5fEfbEWsGmXGFVgqq6HU83U=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue Id="SignatureValue">JFj/qtAzDRgUFpoGuchiwfUGUGkIDHVLLwNGS1e9kLxTkE5PI6oGW2Gp/fWjs6z7
        lyKCFOk69WzonA//F6ae5fELG4VPsQqfhsH7KCV4372oyyyYi+U4o1I72I4Ruxdi
        +qfffeX9rUcnwHbn+lfm6anT85eHIYPo28Es0LACQbmzgDgksk4TIX+x5+0Jpjvt
        qk62IuE1ayHTFp/xb74Qm+LLggRjhM9H2spimHvK5w4b2FguRFgtVlLTcv0s5F1V
        zXdb4RD9bbSlsvYDRUiFJ0kkengtH1r/Q9I5VOLgVrPdAd+5Nyhga855BsnUpo1t
        Aap2uAZvfPplrvmKUh35VQ==</ds:SignatureValue>
```

Figure G.1—The EML SEAL digital signature element, excerpted from "UOCAVA-BBD-example-EML505-*yyyymmdd*.xml"

If an EML file points to another document such as a blank ballot file via a URL, the document SHOULD also be checked when signatures are validated to ensure that it has not changed since it was signed. Such a document SHOULD be listed as a Reference within the Manifest element in the SEAL so that its DigestValue will be computed and stored and included in the data that is signed.

Figure G.2 shows the Manifest element in UOCAVA-BBD-example-EML505-yyyymmdd.xml and shows digital signatures calculated on two blank ballot files (F2Z666-20110607.pdf and F3Y111-20110607.pdf).

```
- <ds:Manifest Id="manifest-20110707112708271-61">
  - <ds:Reference URI="http://grouper.ieee.org/groups/1622/examples/UOCAVA-BBD-example-ballot-F2Z666-
      20110607.pdf">
      <ds:Transforms />
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>MUiJMZsZF98GTkmu0Ndk74E5wouW09zS+V8hEYtRXBk=</ds:DigestValue>
    </ds:Reference>
  - <ds:Reference URI="http://grouper.ieee.org/groups/1622/examples/UOCAVA-BBD-example-ballot-F3Y111-
      20110607.pdf">
      <ds:Transforms />
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>rfxwaPRJR6qy4paVLodxHfxhTnaWQ6QrMUSenslczys=</ds:DigestValue>
    </ds:Reference>
  </ds:Manifest>
```

Figure G.2—The Manifest element within the SEAL element

The aforementioned blank ballot files are subsequently used as references in the body of the EML message under the <*BallotStyleImage*> element's <*URL*> child element (see Annex D, Figure D.2). Note that while certain fields of the <*URL*> element also permit storing a hash code of the referenced file, the <*ds:*> element's fields in the Manifest are specified in W3C's guidance and SHALL be used.

Note that formal guidance on digital signatures is beyond the scope of this document, however some guidelines are noted here for digital signatures to verify properly; see also DRAFT Special Publication 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP) [B12]. In particular, attention will have to be paid to the canonicalization method used (e.g., carefully choosing a method such as Canonical XML 1.1[15]) and the algorithms employed (adherence to FIPS 186-3, Digital Signature Standard [B13] is recommended). The example uses the "embedded signature" method where the whole contents of the file are signed, except of course the signature itself.

[15] See http://www.w3.org/TR/xml-c14n11/#XMLCanonicalization.