THE FUTURE OF VOTING
End-To-End Verifiable Internet Voting

BON Specifications

Joseph R. Kiniry and Daniel M. Zimmerman
Galois

10 July 2015

CONTENTS

ABOUT THIS DOCUMENT

This document is a part of the full report "THE FUTURE OF VOTING: End-To-End Verifiable Internet Voting", available from https://www.usvotefoundation.org/E2E-VIV. It presents a comprehensive domain model and set of requirements for an E2E-VIV system, using the Business Object Notation (BON).

BON, developed by Kim Waldén and Jean-Marc Nerson and described in their 1995 book *Seamless object-oriented software architecture: Analysis and design of reliable systems*, is both a language and a design/refinement method encompassing informal domain analysis and modeling, formal modeling, and implementation-independent high- and medium-level specification. BON has a well-defined semantics, is easy to learn and write (especially the informal models, which are effectively collections of simple English sentences), and has equally-expressive textual and graphical notations. BON was originally developed for use with the Eiffel programming language; however, it can be used with other specification and implementation languages. We use BON for domain modeling for several reasons.

First, BON's equivalently expressive textual and graphical notations are easy to work with and manipulate.

Second, BON's semantics are an integral part of the language and method and are easily understandable.

Third, BON explicitly supports (and encourages) *seamlessness* and *reversibility*. Seamlessness is the property that allows a BON model to be smoothly (and, in many cases, completely automatically) refined to lower-level specification languages, and further to executable implementations. Reversibility is the property that allows consistency to be maintained between the BON model, which is an important part of the system documentation, and the resulting implementation—when the implementation is changed, that change can be (again, often completely automatically) propagated back up to the BON model. Seamlessness and reversibility are both useful properties for ensuring that the final software product accurately reflects the original domain analysis and architecture design.

Fourth, BON supports high-level domain modeling using natural language, making it easy to communicate models not only among software developers but also with other stakeholders in the development process. The BON representation of the E2E-VIV requirements consists almost entirely of simple English sentences; it is therefore far more accessible to a wide audience than an equivalent set of box-and-arrow diagrams would be.

Finally, BON is *simple*. Its specification is small, and it is easy to understand.

CHAPTER 1

BON REPRESENTATION OF E2E-VIV REQUIREMENTS

The following is a comprehensive set of requirements for an E2E-VIV system, in the form of BON specifications. The corresponding BON files are available in the E2E-VIV GitHub repository, at https://github.com/GaloisInc/e2eviv.

1.1 E2EVIV.BON

```
scenario_chart E2EVIV_REQUIREMENTS
indexing
  title: "Requirements for End-to-end Verifiable Internet Voting Systems.";
  editor: "Joe Kiniry <kiniry@galois.com>", "Daniel M. Zimmerman <dmz@galois.com>";
  created: "16 July 2014";
  revised: "April 2015"
explanation
  "Functional and non-functional requirements for end-to-end \
 \ verifiable internet voting systems.  Requirements consisting of two \
 \ or more sentences are in fact stipulating multiple, related \
 \ requirements in a single scenario.  We index requirements from one, \
 \ thus SYSTEM_AND_DATA_ACCESS_CONTROL requirement 1 is 'Only persons \
 \ appointed by the electoral authority shall have access to the \
 \ central infrastructure, the servers and the election data.'."
end
```

1.2 TECHNICAL.BON

```
scenario_chart TECHNICAL_REQUIREMENTS
indexing
  partof: "E2EVIV_REQUIREMENTS";
explanation
  "General technical requirements for digital elections systems."
end
```

1.3 NON-FUNCTIONAL.BON

```
scenario_chart NON_FUNCTIONAL_REQUIREMENTS
indexing
  partof: "E2EVIV_REQUIREMENTS"
explanation
  "General non-functional requirements of digital voting systems."
end
```

1.4 ACCESSIBILITY.BON

```
scenario_chart ACCESSIBILITY_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General requirements for accessibility of digital election systems."

scenario
  "MANDATORY_ACCESSIBILITY_TESTING" -- @ref Kiniry/Zimmerman
description
  "Accessibility testing for disabled and abled voters shall be performed, \
 \ and the reports of the testing made public. The system must achieve \
 \ satisfactory accessibility testing results before being used in a \
 \ binding election."

-- @ref Rec(2004)11 Accessibility
scenario "UNIVERSAL_ACCESSIBILITY" -- @ref Rec(2004)11 Appendix III, A. 61.
description
  "Measures shall be taken to ensure that the relevant software and \
 \ services can be used by all voters and, if necessary, provide access \
 \ to alternative ways of voting."

scenario "ACCESSIBILITY_STAKEHOLDERS" -- @ref Rec(2004)11 Appendix III, A. 62.
description
  "Users shall be involved in the design of e-voting systems, \
 \ particularly to identify constraints and test ease of use at each \
 \ main stage of the development process."

scenario "USER_FACILITIES_FOR_ACCESSIBILITY" -- @ref Rec(2004)11 Appendix III, A. 63.
description
  "Users shall be supplied, whenever required and possible, with \
 \ additional facilities, such as special interfaces or other \
 \ equivalent resources, such as personal assistance."

scenario "COMPLEMENT_ACCESSIBILITY_TECHNOLOGIES" -- @ref Rec(2004)11 Appendix III, A. 64.
description
  "Consideration shall be given, when developing new products, to \
 \ their compatibility with existing ones, including those using \
 \ technologies designed to help people with disabilities."

scenario "ACCESSIBLE_VOTING_OPTIONS" -- @ref Rec(2004)11 Appendix III, A. 65.
description
  "The presentation of the voting options shall be optimised for the \
```

```
 \ voter."
end
```

1.5 ASSURANCE.BON

```
scenario_chart ASSURANCE_REQUIREMENTS
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "General non-functional assurance requirements which increase system \
 \ and election assurance."

scenario
  "CLIENT_ENVIRONMENTS" -- @ref David Jefferson
description
  "Client side software (applications, apps, scripts, etc.) should be \
 \ free of known bugs on a wide range of platform and software stack \
 \ combinations intended to be usable as voting terminals."

scenario
  "AUTHENTICATION_RESILIENCE" -- @ref David Jefferson
description
  "There must be no way to automate forging or invalidation of \
 \ voter authentications without compromising the cryptographic \
 \ protocols or secrets used in the system."

scenario
  "OPEN_DOCUMENTATION" -- @ref David Jefferson
description
  "All aspects of the design, architecture, algorithms and \
 \ documentation for the entire Internet voting system (not just the \
 \ E2EV core) should be published and available for free download by \
 \ anyone."

scenario
  "DOCUMENTATION_CONSISTENCY" -- @ref David Jefferson
description
  "As the system changes, all documentation must be kept up to \
 \ date.  No new version of an E2EV Internet voting system may be \
 \ certified until all documentation is up to date."

scenario
  "OPEN_SOURCE" -- @ref David Jefferson
description
  "The source code, build scripts, issue tracking system, security \
 \ features, and related development information for the entire \
 \ Internet voting system (all versions for all platforms) shall be \
 \ made publicly available for free download and inspection by \
 \ anyone."

scenario
  "SOURCE_LICENSE" -- @ref David Jefferson
description
  "The source code for all parts of the E2EV Internet voting system \
 \ shall be made publicly available under a license that permits \
 \ anyone to download the code and build, instrument, and test it."
```

```
end
```

1.6 AUDITING.BON

```
scenario_chart AUDITING_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General requirements pertaining to auditing systems and digital \
 \ election systems."

-- @ref Rec(2004)11 Audit, I. General
scenario "AUDIT_SYSTEMS" -- @ref Rec(2004)11 Appendix III, E. I. 100.
description
  "The audit system shall be designed and implemented as part of the \
 \ e-voting system.  Audit facilities shall be present on different \
 \ levels of the system: logical, technical and application."

scenario "AUDITING_COMPLETENESS" -- @ref Rec(2004)11 Appendix III, E. I. 101.
description
  "End-to-end auditing of an e-voting system shall include recording, \
 \ providing monitoring facilities and providing verification \
 \ facilities."

-- @ref Rec(2004)11 Audit, II. Recording
scenario "AUDIT_SYSTEM_BASELINE" -- @ref Rec(2004)11 Appendix III, E. II. 102.
description
  "The audit system shall be open and comprehensive, and actively \
 \ report on potential issues and threats."

scenario "AUDIT_SYSTEM_DATA" -- @ref Rec(2004)11 Appendix III, E. II. 103.
description
  "The audit system shall record times, events and actions, including: \
 \ a. all voting-related information, including the number of eligible \
 \ voters, the number of votes cast, the number of invalid votes, the \
 \ counts and recounts, etc.; b. any attacks on the operation of the \
 \ e-voting system and its communications infrastructure; c. system \
 \ failures, malfunctions and other threats to the system."

-- @ref Rec(2004)11 Audit, III. Monitoring
scenario "AUDIT_SYSTEM_EVIDENCE" -- @ref Rec(2004)11 Appendix III, E. III. 104.
description
  "The audit system shall provide the ability to oversee the election \
 \ or referendum and to verify that the results and procedures are in \
 \ accordance with the applicable legal provisions."

scenario "AUDIT_DATA_SECURITY" -- @ref Rec(2004)11 Appendix III, E. IIi. 105.
description
  "Disclosure of the audit information to unauthorized persons shall \
 \ be prevented."

scenario "AUDIT_DATA_SECRECY" -- @ref Rec(2004)11 Appendix III, E. III. 106.
description
  "The audit system shall maintain voter anonymity at all times."
```

```
-- @ref Rec(2004)11 Audit, II. Verifiability
scenario "AUDIT_SYSTEM_CAPABILITY" -- @ref Rec(2004)11 Appendix III, E. IV. 107.
description
  "The audit system shall provide the ability to cross-check and \
 \ verify the correct operation of the e-voting system and the accuracy \
 \ of the result, to detect voter fraud, and to prove that all counted \
 \ votes are authentic and that all votes have been counted."

scenario "AUDIT_SYSTEM_FOR_LEGAL_COMPLIANCE" -- @ref Rec(2004)11 Appendix III, E. IV. 108.
description
  "The audit system shall provide the ability to verify that an \
 \ e-election or e-referendum has complied with the applicable legal \
 \ provisions."

-- @ref Rec(2004)11 Audit, II. Other
scenario "AUDIT_DATA_VALIDITY" -- @ref Rec(2004)11 Appendix III, E. V. 109.
description
  "The audit system shall be protected against attacks that may \
 \ corrupt, alter or lose records in the audit system."

scenario "AUDIT_DATA_CONFIDENTIALITY" -- @ref Rec(2004)11 Appendix III, E. V. 110.
description
  "The electoral authority shall take adequate steps to ensure that the \
 \ confidentiality of any information obtained by any person while \
 \ carrying out auditing functions is guaranteed."

scenario
  "LOG_BASICS" -- @ref David Jefferson
description
  "The Internet voting system should keep detailed logs of all \
 \ relevant activity."

scenario
  "LOG_IMMUTABILITY" -- @ref David Jefferson
description
  "Log entries must be unmodifiable once written."

scenario
  "LOG_COMMITMENT" -- @ref Ron Rivest
description
  "Log entries must accurately reflect the commitment character \
 \ of elections and the relationships among election events \
 \ (e.g., ballot, vote, voter, and election state transitions)."

scenario
  "LOG_DATA_COMPLETENESS" -- @ref David Jefferson
description
  "The log data should be as complete as possible, consistent with \
 \ maximum possible vote privacy."

scenario
  "PRIVACY_VS_FRAUD_TRADEOFF" -- @ref David Jefferson
description
  "If there is a tradeoff between vote privacy and the identification \
 \ of the perpetrators of fraud, the decision should be made in favor \
 \ of vote privacy."

scenario
  "VOTER_LIST" -- @ref David Jefferson
```

```
description
  "The list of voters who voted online should be published."
end

scenario_chart AUDITING_REQUIREMENTS_VERIFICATION
indexing
  partof: "AUDITING_REQUIREMENTS"
explanation
  "Requirements specific to auditing verifiable elections."

scenario
  "VERIFICATION_PARTIAL_FAILURE" -- @ref David Jefferson
description
  "The system, in the event that it does not verify the online \
 \ votes cast, must be capable of giving an upper bound on the \
 \ number of ballots that may have been affected."

scenario
  "VERIFICATION_SOURCE" -- @ref David Jefferson
description
  "Official verification applications, like the voting software itself, \
 \ must be published in source form along with documentation, build \
 \ directions, and a standard cryptographic hash of the source code."
end
```

1.7 AUTHENTICATION.BON

```
scenario_chart AUTHENTICATION_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General requirements relating to the authentication of principles \
 \ (both computers and humans) involved in any digital election \
 \ system."

scenario
  "VOTER_AUTHENTICATION" -- @ref David Jefferson
description
  "The voting service must by itself securely authenticate the voter \
 \ (verify identify the voter and verify his/her registration and/or \
 \ eligibility according to law to vote in the election) before \
 \ allowing him/her to cast a ballot (or modify or replace a \
 \ previously cast ballot)."

scenario
  "NO_THIRD_PARTY_AUTHENTICATION" -- @ref David Jefferson
description
  "Authentication must not be done through third party intermediaries \
 \ such as Facebook, iCloud, Google, Yahoo, Amazon, etc. that offer \
 \ authentication services."

scenario
  "SECRET_AUTHENTICATION_SHARED_SECRETS" -- @ref David Jefferson
description
  "Authentication for remote voting systems must not use personal \
 \ information, government or commercial account identifiers, etc."
```

```
scenario
  "AUTHENTICATION_DATA_UPDATES" -- @ref David Jefferson
description
  "Authentication secrets must be changeable or revokable at \
 \ any time at the behest of either the voter or election \
 \ officials."

scenario
  "AUTHENTICATION_DATA_REFRESH_PERIODICITY" -- @ref David Jefferson
description
  "All voter authentication secrets must be changed at least once in \
 \ every election cycle."

end
```

1.8 CERTIFICATION.BON

```
scenario_chart CERTIFICATION_FUNCTIONAL_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "Requirements relating to the functional certification of digital \
 \ election systems and elections."

scenario "AUTOMATED_TESTING" -- @ref Kiniry/Zimmerman
description
  "Each functional requirement must have an associated set of automated \
 \ tests that provide evidence that the requirement is fulfilled."

scenario "ELECTION_PROTOCOL_PROOFS" -- @ref Kiniry/Zimmerman
description
  "The election protocol shall have associated formal proofs of correctness \
 \ and security."
end

scenario_chart CERTIFICATION_NON_FUNCTIONAL_REQUIREMENTS
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "Requirements relating to the non-functional certification of \
 \ election systems and elections."

-- @ref Rec(2004)11 Certification
scenario "CERTIFICATION_PROCESSES" -- @ref Rec(2004)11 Appendix III, F. 111.
description
  "The electoral authority shall introduce certification processes that allow \
 \ for any ICT (Information and Communication Technology) component to \
 \ be tested and certified as being in conformity with technical \
 \ requirements."

scenario
  "CERTIFICATION_PARTIES_COMPETENCE" -- @ref David Jefferson
description
  "Any E2EV Internet voting system should be certified by competent \
 \ professionals."
```

```
scenario
  "CERTIFICATION_REPORT_TRANSPARENCY" -- @ref David Jefferson
description
  "Any and all certification reports issued by certification \
 \ professionals must be public, whether they recommend \
 \ certification or not."

scenario
  "RECERTIFICATION_CONDITIONS" -- @ref David Jefferson
description
  "Any time there is a change in the voting system client or server \
 \ side or the E2EV system, all of the requirements must \
 \ be re-established and recertified.  Changes that mandate \
 \ re-certification include, but are not limited to: new supported \
 \ hardware platforms, OS's, browsers, etc.; bug fixes and security \
 \ patches to voting client and/or server; changes or upgrades to \
 \ voting client or server in response to detected bugs or security \
 \ vulnerabilities, changes in law, or changes in threat environment."

scenario
  "RECERTIFICATION_PERIODICITY" -- @ref David Jefferson
description
  "The requirements must be re-established and recertified every \
 \ election cycle even if there are no changes."

scenario
  "VALIDATION_PLATFORM_COVERAGE" -- @ref David Jefferson
description
  "The system must be extensively tested on a wide range of platform \
 \ and software combinations."

scenario
  "PUBLIC_VALIDATION_PLATFORM_COVERAGE_RESULTS" -- @ref David Jefferson
description
  "All test procedures and results for platform coverage must be public."

end
```

1.9 EVOLVABILITY.BON

```
scenario_chart EVOLVABILITY_REQUIREMENTS
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "General requirements on the evolvability of digital election \
 \ systems."

scenario
  "ELECTORAL_AUTHORITY_UPDATE"
description
  "The electoral authority has the right and ability to update \
 \ election systems to conform to changes in applicable law, \
 \ available techology, or the system threat model."

end
```

1.10 FUNCTIONAL.BON

```
scenario_chart FUNCTIONAL_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General functional requirements for digital election systems."

scenario
  "CASTING_ATOMIC" -- @ref David Jefferson
description
  "Ballot casting shall be atomic with respect to server failures."

scenario
  "DETERMINISTIC_VOTING_PROCESS" -- @ref David Jefferson
description
  "If a server side failure occurs, no voter's balloting can be \
 \ left in an unknown state."

scenario
  "BALLOT_FINAL_STATES" -- @ref David Jefferson
description
  "Either a ballot is securely and completely cast and the \
 \ voter is marked as having voted, or no ballot is recorded and the \
 \ voter is not marked as having voted."

scenario
  "VOTE_RECORD_MONOTONICITY" -- @ref David Jefferson
description
  "If the system and the law allows a voter to cast multiple votes \
 \ with only the last one counting, or to cast a partial ballot with \
 \ the option of modifying it later, then each voting session must be \
 \ atomic with respect to server failures. If a failure occurs during the \
 \ voter's last session, then the votes cast as of his or her previous \
 \ session will count."

scenario
  "RECEIPT_FREEDOM" -- @ref David Jefferson
description
  "There must be no way for voters to prove to another party any \
 \ information regarding how they voted in any race (beyond what is \
 \ mathematically deducible from the final distribution of votes)."

scenario
  "VALID_BALLOT_PROVENANCE" -- @ref David Jefferson
description
  "Once it is determined that a ballot will be counted, the ballot \
 \ shall be irrevocably separated from the identification of the \
 \ voter who cast it."

scenario
  "MULTI_BALLOT_RECORD" -- @ref David Jefferson
description
  "If the voting system permits voters to modify or replace their \
 \ previously cast ballots, only the latest vote by each voter in \
 \ each race shall be counted in the final tally."
```

```
scenario
  "NO_DOUBLE_VOTE" -- @ref David Jefferson
description
  "But for systems supporting MULTI_BALLOT_RECORD, the voting system \
 \ shall not record more than one vote for any voter in any race."

scenario
  "NO_ADVERTISING" -- @ref David Jefferson
description
  "The voting system client must not display or permit the display of \
 \ any advertising or commercial logos in the window that contains the \
 \ voting session, other than those of the election jurisdiction \
 \ itself."

scenario
  "NO_EXTERNAL_LINKS" -- @ref David Jefferson
description
  "The voting system client must not display any links to other sites \
 \ except for help in the mechanics of voting."

end
```

1.11 INTEROPERABILITY.BON

```
scenario_chart INTEROPERABILTY_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General requirements on the interoperability of digital election \
 \ systems."

-- @ref Rec(2004)11 Interoperabilty
scenario "OPEN_STANDARDS" -- @ref Rec(2004)11 Appendix III, B. 66.
description
  "Open standards shall be used to ensure that the various technical \
 \ components or services of an e-voting system, possibly derived \
 \ from a variety of sources, interoperate."

scenario "EML" -- @ref Rec(2004)11 Appendix III, B. 67.
description
  "The Election Markup Language (EML) shall be used whenever possible \
 \ for e-election and e-referendum applications."

scenario "DATA_LOCALIZATION" -- @ref Rec(2004)11 Appendix III, B. 68.
description
  "In cases that imply specific election or referendum data \
 \ requirements, a localization procedure shall be used to accommodate \
 \ these needs."

scenario
  "OPEN_LOG_FORMATS" -- @ref David Jefferson
description
  "The log data and documentation of its meaning and format shall be \
 \ available for public download so that anyone can download, inspect, \
 \ and publish concerns based on the logs."
```

```
end
```

1.12 LEGAL.BON

```
scenario_chart LEGAL_REQUIREMENTS
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "General legal requirements relating to legal matters and digital \
 \ election systems."

-- @ref Rec(2004)11 Universal Suffrage
scenario -- @ref Rec(2004)11 Appendix I, A. I. 1.
  "USABLE_UI"
description
  "The voter interface of an e-voting system shall be understandable and \
 \ easily usable."

scenario -- @ref Rec(2004)11 Appendix I, A. I. 2.
  "UNIMPEDED_REGISTRATION"
description
  "Possible registration requirements for e-voting shall not pose \
 \ an impediment to the voter participating in e-voting."

scenario -- @ref Rec(2004)11 Appendix I, A. I. 3.
  "MAXIMIZE_DISABLED_ACCESSIBILITY"
description
  "E-voting systems shall be designed, as far as it is practicable, to \
 \ maximize the opportunities that such systems can provide for persons \
 \ with disabilities."

scenario -- @ref Rec(2004)11 Appendix I, A. I. 4.
  "REMOTE_ONLY_SUPPLEMENTARY"
description
  "Unless channels of remote e-voting are universally accessible, they \
 \ shall be only an additional and optional means of voting."

-- @ref Rec(2004)11 Equal suffrage
scenario -- @ref Rec(2004)11 Appendix I, A. II. 5--6.
  "AT_MOST_ONE_VOTE_PER_VOTER"
description
  "The e-voting system shall ensure that at most one electronic vote from \
 \ each voter is included in the final tally."

scenario -- @ref Rec(2004)11 Appendix I, A. II. 7.
  "VALID_TALLY"
description
  "Every vote deposited in an electronic ballot box shall be counted, and \
 \ each vote cast in the election or referendum shall be counted only once."

scenario -- @ref Rec(2004)11 Appendix I, A. II. 8.
  "VOTE_AGGREGATION"
description
  "Where electronic and non-electronic voting channels are used in the same \
 \ election or referendum, there shall be a secure and reliable method to \
 \ aggregate all votes and to calculate the correct result."
```

```
-- @ref Rec(2004)11 Free suffrage
scenario -- @ref Rec(2004)11 Appendix I, A. III. 9.
  "FREE_SUFFRAGE"
description
  "The organization of e-voting shall secure the free formation and \
 \ expression of the voter's opinion and, where required, the \
 \ personal exercise of the right to vote."

scenario -- @ref Rec(2004)11 Appendix I, A. III. 10.
  "REFLECTIVE_VOTING_PROCESS"
description
  "The way in which voters are guided through the e-voting process \
 \ shall be such as to prevent their voting precipitately or without \
 \ reflection."

scenario -- @ref Rec(2004)11 Appendix I, A. III. 11.
  "FLEXIBLE_VOTING_PROCESS"
description
  "Voters shall be able to alter their choice at any point in the \
 \ e-voting process before casting their vote, or to break off the \
 \ procedure, without their previous choices being recorded or made \
 \ available to any other person."

scenario -- @ref Rec(2004)11 Appendix I, A. III. 12.
  "NO_VOTER_MANIPULATION"
description
  "The e-voting system shall not permit any manipulative influence to \
 \ be exercised over the voter during the voting."

scenario -- @ref Rec(2004)11 Appendix I, A. III. 13.
  "BLANK_VOTE"
description
  "The e-voting system shall provide the voter with a means of \
 \ participating in an election or referendum without the voter \
 \ exercising a preference for any of the voting options, for example, \
 \ by casting a blank vote."

scenario -- @ref Rec(2004)11 Appendix I, A. III. 14.
  "CONCLUSION_OF_VOTING_PROCESS"
description
  "The e-voting system shall indicate clearly to the voter when the \
 \ vote has been cast successfully and when the whole voting procedure \
 \ has been completed."

scenario -- @ref Rec(2004)11 Appendix I, A. III. 15.
  "IMMUTABLE_VOTES"
description
  "Except in systems supporting MULTI_BALLOT_RECORD, the e-voting system \
 \ shall prevent the changing of a vote once that vote has been cast."

-- @ref Rec(2004)11 Secret suffrage
scenario -- @ref Rec(2004)11 Appendix I, A. IV. 16.
  "SECRET_SUFFRAGE"
description
  "E-voting shall be organized in such a way as to exclude at any \
 \ stage of the voting procedure and, in particular, at voter \
 \ authentication, anything that would endanger the secrecy of the \
 \ vote."
```

```
scenario -- @ref Rec(2004)11 Appendix I, A. IV. 17.
  "ANONYMOUS_VOTES"
description
  "The e-voting system shall guarantee that votes in the electronic \
 \ ballot box and votes being counted are, and will remain, anonymous, \
 \ and that it is not possible to reconstruct a link between the vote \
 \ and the voter."

scenario -- @ref Rec(2004)11 Appendix I, A. IV. 18.
  "NO_INDIRECT_SECRECY_VIOLATION"
description
  "The e-voting system shall be so designed that the expected number \
 \ of votes in any electronic ballot box will not allow the result to \
 \ be linked to individual voters."

scenario -- @ref Rec(2004)11 Appendix I, A. IV. 19.
  "NO_SECRET_SUFFRAGE_SIDE_CHANNEL"
description
  "Measures shall be taken to ensure that the information needed \
 \ during electronic processing cannot be used to breach the secrecy of \
 \ the vote."

scenario
  "NO_NDAS_FOR_STUDY" -- @ref David Jefferson 22-6-2014
description
  "No nondisclosure agreement or any other contract shall be required \
 \ to download and study the Internet voting system."

scenario
  "NO_NDAS_FOR_AUDIT" -- @ref David Jefferson 22-6-2014
description
  "No nondisclosure agreement or any other contract shall be required \
 \ to download, instrument, build, test, and publish test results for \
 \ an E2EV Internet voting system."

end
```

1.13 MAINTENANCE.BON

```
scenario_chart MAINTENANCE_REQUIREMENTS
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "General requirements relating to the maintainence of digital election \
 \ systems."

scenario
  "ELECTORAL_AUTHORITY_PATCH"
description
  "The electoral authority has the right and ability to patch \
 \ election systems to correct flaws discovered in the algorithms, \
 \ implementation, or deployment."

end
```

1.14 OPERATIONAL.BON

```
scenario_chart OPERATIONAL_REQUIREMENTS
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "General operational requirements for digital election systems."

-- @ref Rec(2004)11 Notification
scenario "ELECTION_TIMETABLES" -- @ref Rec(2004)11 Appendix II, I. 36.
description
  "Domestic legal provisions governing an e-election or e-referendum \
 \ shall provide for clear timetables concerning all stages of the \
 \ election or referendum, both before and after the election or \
 \ referendum."

scenario "ELECTION_PERIOD" -- @ref Rec(2004)11 Appendix II, I. 37.
description
  "The period in which an electronic vote can be cast shall not begin \
 \ before the notification of an election or a referendum.  Particularly \
 \ with regard to remote e-voting, the period shall be defined and made \
 \ known to the public well in advance of the start of voting."

scenario "EVOTING_OUTREACH" -- @ref Rec(2004)11 Appendix II, I. 38.
description
  "The voters shall be informed, well in advance of the start of \
 \ voting, in clear and simple language, of the way in which the \
 \ e-voting will be organised, and any steps a voter may have to take \
 \ in order to participate and vote."

-- @ref Rec(2004)11 Voters
scenario "VOTER_VERIFIABLE_VOTER_REGISTER" -- @ref Rec(2004)11 Appendix II, II. 39.
description
  "There shall be a voters' register that is regularly updated.  The \
 \ voter shall be able to check, as a minimum, the information that is \
 \ held about him/her on the register, and request corrections."

scenario "ONLINE_VOTER_REGISTER" -- @ref Rec(2004)11 Appendix II, II. 40.
description
  "The possibility of creating an electronic register and introducing \
 \ a mechanism allowing online application for voter registration \
 \ and, if applicable, for application to use e-voting, shall be \
 \ considered.  If participation in e-voting requires a separate \
 \ application by the voter and/or additional steps, an electronic, \
 \ and, where possible, interactive procedure shall be considered."

scenario "VOTER_REGISTRATION_ELECTION_OVERLAP" -- @ref Rec(2004)11 Appendix II, II. 41.
description
  "In cases where there is an overlap between the period for voter \
 \ registration and the voting period, provision for appropriate \
 \ voter authentication shall be made."

-- @ref Rec(2004)11 Candidates
scenario "ONLINE_CANDIDATE_NOMINATION" -- @ref Rec(2004)11 Appendix II, III. 42.
description
  "The possibility of introducing online candidate nomination may be \
```

```
 \ considered."

scenario "PUBLIC_CANDIDATE_LIST" -- @ref Rec(2004)11 Appendix II, III. 43.
description
  "A list of candidates that is generated and made available \
 \ electronically shall also be publicly available by other means."

-- @ref Rec(2004)11 Voting
scenario "MULTIPLE_CHANNELS_ONE_VOTE" -- @ref Rec(2004)11 Appendix II, IV. 44.
description
  "Where remote e-voting takes place while polling stations are open, \
 \ the system shall be so designed that it prevents any voter from \
 \ voting more than once."

scenario "VOTING_PERIOD_INVARIANT" -- @ref Rec(2004)11 Appendix II, IV. 45.
description
  "Remote e-voting may start and/or end at an earlier time than the \
 \ opening of any polling station.  Remote e-voting shall not continue \
 \ after the end of the voting period at polling stations."

scenario "UNIVERSAL_VOTER_HELP" -- @ref Rec(2004)11 Appendix II, IV. 46.
description
  "For every e-voting channel, support and guidance arrangements on \
 \ voting procedures shall be set up for, and be available to, the \
 \ voter.  In the case of remote e-voting, such arrangements shall also \
 \ be available through a different, widely-available communication \
 \ channel."

scenario "FAIR_VOTING_OPTIONS" -- @ref Rec(2004)11 Appendix II, IV. 47.
description
  "There shall be equality in the manner of presentation of all voting \
 \ options on the device used for casting an electronic vote."

scenario "VOTING_OPTIONS_ONLY" -- @ref Rec(2004)11 Appendix II, IV. 48.
description
  "The electronic ballot by which an electronic vote is cast shall be \
 \ free from any information about voting options, other than that \
 \ strictly required for casting the vote.  The e-voting system shall \
 \ avoid the display of other messages that may influence the voters' \
 \ choice."

scenario "FAIR_VOTING_OPTION_INFORMATION" -- @ref Rec(2004)11 Appendix II, IV. 49.
description
  "If it is decided that information about voting options will be \
 \ accessible from the e-voting site, this information shall be \
 \ presented with equality."

scenario "BINDING_ELECTION_CLARITY" -- @ref Rec(2004)11 Appendix II, IV. 50.
description
  "Before casting a vote using a remote e-voting system, voters' \
 \ attention shall be explicitly drawn to the fact that the e-election \
 \ or e-referendum in which they are submitting their decision by \
 \ electronic means is a real election or referendum.  In case of \
 \ tests, participants shall have their attention drawn explicitly to \
 \ the fact that they are not participating in a real election or \
 \ referendum and shall, when tests are continued at election times, \
 \ at the same time be invited to cast their ballot by the voting \
 \ channel(s) available for that purpose."
```

```
scenario "REMOTE_RECEIPT_FREEDOM" -- @ref Rec(2004)11 Appendix II, IV. 51.
description
  "A remote e-voting system shall not enable the voter to be in \
 \ possession of a proof of the content of the vote cast."

scenario "SUPERVISED_VOTE_RECEIPT_FREEDOM" -- @ref Rec(2004)11 Appendix II, IV. 52.
description
  "In a supervised environment, the information on the vote shall \
 \ disappear from the visual, audio or tactile display used by the \
 \ voter to cast the vote as soon as it has been cast.  Where a paper \
 \ proof of the electronic vote is provided to the voter at a polling \
 \ station, the voter shall not be able to show it to any other per- \
 \ son, or take this proof outside of the polling station."

-- @ref Rec(2004)11 Results
scenario "SECRET_INTERMEDIATE_TALLY" -- @ref Rec(2004)11 Appendix II, V. 53.
description
  "The e-voting system shall not allow the disclosure of the number of \
 \ votes cast for any voting option until after the closure of the \
 \ electronic ballot box.  This information shall not be disclosed to \
 \ the public until after the end of the voting period."

scenario "NO_ITALIAN_ATTACK" -- @ref Rec(2004)11 Appendix II, V. 54.
description
  "The e-voting system shall prevent processing information on votes \
 \ cast within deliberately chosen sub-units that could reveal \
 \ individual voters' choices."

scenario "DECODING_LATENCY" -- @ref Rec(2004)11 Appendix II, V. 55.
description
  "Any decoding required for the counting of the votes shall be \
 \ carried out as soon as practicable after the closure of the voting \
 \ period."

scenario "TALLY_OBSERVATION" -- @ref Rec(2004)11 Appendix II, V. 56.
description
  "When counting the votes, representatives of the competent electoral \
 \ authority shall be able to participate in, and any observers able to \
 \ observe, the count."

scenario "TALLY_RECORD" -- @ref Rec(2004)11 Appendix II, V. 57.
description
  "A record of the counting process of the electronic votes shall be \
 \ kept, including information about the start and end of, and the \
 \ persons involved in, the count."

scenario "INTEGRITY_VIOLATION_RECORD" -- @ref Rec(2004)11 Appendix II, V. 58.
description
  "In the event of any irregularity affecting the integrity of votes, \
 \ the affected votes shall be recorded as having their integrity violated."

-- @ref Rec(2004)11 Audit
scenario "SYSTEM_AUDITABILITY" -- @ref Rec(2004)11 Appendix II, VI. 59.
description
  "The e-voting system shall be auditable."

scenario "SYSTEM_AUDITS_IMPACT" -- @ref Rec(2004)11 Appendix II, VI. 60.
description
  "The conclusions drawn from the audit process shall be applied in \
```

```
 \ future elections and referenda."

scenario
  "OPEN_SYSTEM" -- @ref David Jefferson
description
  "The e-voting system must function correctly as an open system, \
 \ where large parts (the mix of client hardware and software in \
 \ fact) are unknown, unsecured, uncertified, and completely out \
 \ of control of election officials."

scenario
  "SUPPORTED_CLIENTS" -- @ref David Jefferson
description
  "Operators of voting systems must document exactly what client \
 \ configurations are required or supported, including: \
 \  - versions of hardware platforms (PCs, mobile devices, etc.) \
 \  - versions of specific operating systems for those platforms \
 \  - versions of specific browsers, plugins, protocols, or \
 \    other software applications, apps, components, and plugins."

scenario
  "CLIENT_INTERFERENCE" -- @ref David Jefferson
description
  "Operators of voting systems must document exactly which common \
 \ components, plugins, or other software interfere with voting (e.g., \
 \ flash blockers, popup blockers, script blockers, etc.)."

scenario
  "MANDATORY_CLIENT_TECHNOLOGY" -- @ref David Jefferson
description
  "Operators of voting systems must document exactly what configuration \
 \ choices the voter must make to successfully vote (e.g., mandate \
 \ Javascript)."

scenario
  "PRIVACY_ENHANCING_VOTER_OPTIONS" -- @ref David Jefferson
description
  "Operators of voting systems must document exactly what configuration \
 \ choices the voter might wish to make to more strongly protect \
 \ his/her vote privacy; e.g., disable cookies, run privacy-protecting \
 \ browser plugins, vote from virtual machine that is later destroyed, \
 \ log out of social networks, disable remote control and remote \
 \ administration tools, disable incoming connections, etc."

scenario
  "BREADCRUMBS_USER_ADVICE" -- @ref David Jefferson
description
  "Users may be advised to turn off browser history data, cookies, \
 \ logging data, and other tools that might retain a record of the \
 \ vote transaction whether the vote data itself or metadata."

end
```

1.15 PROCEDURAL.BON

```
scenario_chart PROCEDURAL_REQUIREMENTS
```

```
indexing
  partof: "NON_FUNCTIONAL_REQUIREMENTS"
explanation
  "General procedural requirements for digital electoin systems."

-- @ref Rec(2004)11 Transparency
scenario "VOTER_COMPREHENSION_AND_CONFIDENCE" -- @ref Rec(2004)11 Appendix I, B. I. 20.
description
  "The electoral authority shall take steps to ensure that voters understand and \
 \ have confidence in the e-voting system in use."

scenario "PUBLIC_SYSTEM_FUNCTION" -- @ref Rec(2004)11 Appendix I, B. I. 21.
description
  "Information on the functioning of an e-voting system shall be made \
 \ publicly available."

scenario "VOTER_PRACTICE" -- @ref Rec(2004)11 Appendix I, B. I. 22.
description
  "Voters shall be provided with an opportunity to practice any new \
 \ method of e-voting before, and separately from, the moment of \
 \ casting an electronic vote."

scenario "OBSERVER_INVARIANTS" -- @ref Rec(2004)11 Appendix I, B. I. 23.
description
  "Any observers, to the extent permitted by law, shall be able to be \
 \ present to observe and comment on the e-elections, including the \
 \ establishing of the results."

-- @ref Rec(2004)11 Verifiability and accountability
scenario "DISCLOSURE_OBLIGATIONS" -- @ref Rec(2004)11 Appendix I, B. II. 24.
description
  "The components of the e-voting system shall be disclosed, at least \
 \ to the competent electoral authorities, as required for verification \
 \ and certification purposes."

scenario "CERTIFICATION_OBLIGATIONS" -- @ref Rec(2004)11 Appendix I, B. II. 25.
description
  "Before any e-voting system is introduced, and at appropriate \
 \ intervals thereafter, and in particular after any changes are made \
 \ to the system, an independent body, appointed by the electoral \
 \ authorities, shall verify that the e-voting system is working \
 \ correctly and that all the necessary security measures have been \
 \ taken."

scenario "RECOUNT_SUPPORTED" -- @ref Rec(2004)11 Appendix I, B. II. 26.
description
  "There shall be the possibility for a recount.  Other features of the \
 \ e-voting system that may influence the correctness of the results \
 \ shall be verifiable."

scenario "RERUN_SUPPORTED" -- @ref Rec(2004)11 Appendix I, B. II. 27.
description
  "The e-voting system shall not prevent the partial or complete \
 \ re-run of an election or a referendum."

-- @ref Rec(2004)11 Reliability and security
scenario "RELIABILITY_AND_SECURITY" -- @ref Rec(2004)11 Appendix I, B. III. 28.
description
  "The electoral authority shall ensure the reliability and \
```

```
 \ security of the e-voting system."

scenario "NO_FRAUD_OR_INTERVENTION" -- @ref Rec(2004)11 Appendix I, B. III. 29.
description
  "All possible steps shall be taken to avoid the possibility of fraud \
 \ or unauthorized intervention affecting the system during the whole \
 \ voting process."

scenario "SYSTEM_AVAILABILITY" -- @ref Rec(2004)11 Appendix I, B. III. 30.
description
  "The e-voting system shall contain measures to preserve the \
 \ availability of its services during the e-voting process.  It shall \
 \ resist, in particular, malfunction, breakdowns or denial of service \
 \ attacks."

scenario "SYSTEM_GENUINE_AND_CORRECT" -- @ref Rec(2004)11 Appendix I, B. III. 31.
description
  "Before any e-election or e-referendum takes place, the competent \
 \ electoral authority shall satisfy itself that the e-voting system \
 \ is genuine and operates correctly."

scenario "SYSTEM_AND_DATA_ACCESS_CONTROL" -- @ref Rec(2004)11 Appendix I, B. III. 32.
description
  "Only persons appointed by the electoral authority shall have access \
 \ to the central infrastructure, the servers and the election \
 \ data.  There shall be clear rules established for such \
 \ appointments.  Critical technical activities shall be carried out by \
 \ teams of at least two people.  The composition of the teams shall be \
 \ regularly changed.  As far as possible, such activities shall be \
 \ carried out outside election periods."

scenario "OPEN_BALLOT_BOX_INVARIANTS" -- @ref Rec(2004)11 Appendix I, B. III. 33.
description
  "While an electronic ballot box is open, any authorised intervention \
 \ affecting the system shall be carried out by teams of at least two \
 \ people, be the subject of a report, and be monitored by \
 \ representatives of the competent electoral authority and any \
 \ election observers."

scenario "VOTES_INVARIANTS" -- @ref Rec(2004)11 Appendix I, B. III. 34.
description
  "The e-voting system shall maintain the availability and integrity \
 \ of the votes.  It shall also maintain the confidentiality of the \
 \ votes and keep them sealed until the counting process.  If stored or \
 \ communicated outside controlled environments, the votes shall be \
 \ encrypted."

scenario "SEALED_VOTES_VOTER_RELATION" -- @ref Rec(2004)11 Appendix I, B. III. 35.
description
  "Votes and voter information shall remain sealed as long as the data \
 \ is held in a manner where they can be associated.  Authentication \
 \ information shall be separated from the voter's decision at a \
 \ pre-defined stage in the e-election or e-referendum."

scenario
  "VERIFICATION_FAILURE_PROCEDURES" -- @ref David Jefferson
description
  "There must be clear technical and legal procedures for how to \
 \ proceed in the event that voters can prove that their votes were \
```

```
 \ not received accurately or counted, or if the official election \
 \ verification application does not verify that the Internet part of \
 \ the election was correct."

end
```

1.16 SYSTEM_OPERATIONAL.BON

```
scenario_chart SYSTEM_OPERATIONAL_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General system operational requirements for digital election \
 \ systems."

-- @ref Rec(2004)11 Systems Operation
scenario "PUBLIC_SYSTEM_MANIFEST" -- @ref derived from Rec(2004)11 Appendix III, C. 69.
description
  "The electoral authority shall publish an official manifest of the \
 \ software used in an e-election or e-referendum.  At the very least \
 \ the manifest shall indicate the software used, the versions, its date \
 \ of installation and a brief description. A procedure shall be established \
 \ for updating the manifest to reflect changes to the installed software."

scenario "MANIFEST_ACCURACY" -- @ref derived from Rec(2004)11 Appendix III, C. 69.
description
  "It shall be possible for the electoral authority to check the installed \
 \ software against the system manifest at any time."

scenario "SYSTEM_FAILOVER_INVARIANTS" -- @ref Rec(2004)11 Appendix III, C. 70.
description
  "Those responsible for operating the equipment shall draw up a \
 \ contingency procedure for system failures.  Any backup system shall \
 \ conform to the same standards and requirements as the original system."

scenario "DATA_BACKUP_INVARIANTS" -- @ref Rec(2004)11 Appendix III, C. 71.
description
  "Sufficient backup arrangements shall be in place and be permanently \
 \ available to ensure that voting proceeds smoothly.  The staff \
 \ concerned shall be ready to intervene rapidly according to a \
 \ procedure drawn up by the electoral authority."

scenario "SYSTEM_INVARIANTS_DURING_ELECTION" -- @ref Rec(2004)11 Appendix III, C. 72.
description
  "Those responsible for the equipment shall use special procedures to \
 \ ensure that during the polling period the voting equipment and its \
 \ use satisfy requirements.  The backup services shall be regularly \
 \ monitored."

scenario "PRE_ELECTION_CERTIFICATION_INVARIANTS" -- @ref Rec(2004)11 Appendix III, C. 73.
description
  "Before each election or referendum, the equipment shall be checked \
 \ and approved in accordance with a protocol drawn up by the \
 \ electoral authority.  The equipment shall be checked to ensure that \
 \ it complies with technical specifications.  The findings shall be \
 \ submitted to the electoral authority."
```

```
scenario "FORMAL_CONTROL_PROCEDURE" -- @ref Rec(2004)11 Appendix III, C. 74.
description
  "All technical operations shall be subject to a formal control \
 \ procedure.  Any substantial changes to key equipment shall be \
 \ performed with advance notice."

scenario "PHYSICAL_SECURITY_OF_SYSTEMS_INVARIANTS" -- @ref Rec(2004)11 Appendix III, C. 75.
description
  "Key e-election or e-referendum equipment shall be located in a \
 \ secure area and that area shall, throughout the election or \
 \ referendum period, be guarded against interference of any sort and \
 \ from any person.  During the election or referendum period a \
 \ physical disaster recovery plan shall be in place.  Furthermore, any \
 \ data retained after the election or referendum period shall be \
 \ stored securely."

scenario "INCIDENT_RESPONSE_INVARIANTS" -- @ref Rec(2004)11 Appendix III, C. 76.
description
  "Where incidents that could threaten the integrity of the system \
 \ occur, those responsible for operating the equipment shall \
 \ immediately inform the electoral authority, which will \
 \ take the necessary steps to mitigate the effects of the \
 \ incident.  The level of incident that shall be reported shall be \
 \ specified in advance by the electoral authority."

scenario "OPERATIONAL_TRANSPARENCY" -- @ref Kiniry/Zimmerman
description
  "A report containing every manifest change, every data or system \
 \ invariant violation, every control procedure violation, and every \
 \ physical security violation shall be prepared and made public by \
 \ the electoral authority after every election."

end
```

1.17 RELIABILITY.BON

```
scenario_chart RELIABILITY_REQUIREMENTS
indexing
  partof: "SYSTEM_OPERATIONAL_REQUIREMENTS"
explanation
  "General reliability requirements for any internet election system."

scenario
  "GENERAL_MTBF" -- @ref David Jefferson
description
  "The entire voting service (server side) must have a proven MTBF of \
 \ >168 hours (1 week) under peak expected voting loads the entire \
 \ time."

scenario
  "LIVE_ELECTION_MTBF" -- @ref David Jefferson
description
  "MTBF validation must be demonstrated in multiple tests of \
 \ actual mock elections."
```

```
scenario
  "MTBF_CONTRA_DDOS" -- @ref David Jefferson
description
  "MTBF requirements apply only during normal peak operation, not \
 \ during attacks (e.g., DDoS)."

scenario
  "SYSTEM_RECOVERY_TIME" -- @ref David Jefferson
description
  "If service goes down for any reason other than regional natural \
 \ disaster or malicious attack, service must be restored in no more \
 \ than 10 minutes."

scenario
  "UPTIME" -- @ref David Jefferson
description
  "The system must have three nines (99.9%) uptime."

scenario
  "FAILURE_VALIDATION" -- @ref David Jefferson
description
  "Uptime must be demonstrated by failures in actual mock election \
 \ situations, e.g. tested by sudden loss of power to any server."

scenario
  "MIRRORED_FAILOVER_SERVICE" -- @ref David Jefferson
description
  "The system must have a warm spare in a second data center that can take \
 \ over in case of major failure."

scenario
  "FAILOVER_STAFFING" -- @ref David Jefferson
description
  "The system must be staffed at all times to guarantee the 10 minute \
 \ recovery time."

scenario
  "OPERATION_UNDER_DDOS" -- @ref David Jefferson
description
  "In a federal election the voting system must remain available even \
 \ during a large distributed denial of service attack.  It must be \
 \ able to continue correct operation during a sustained DDoS attack \
 \ on any combination of server side IP addresses (whether at the \
 \ primary server data center or its ISP) at a total level of 100 Gb/s \
 \ with no more than 15s degradation of response time to voters during \
 \ the attack."

scenario
  "DDOS_REFRESH_PERIODICITY" -- @ref David Jefferson
description
  "The DDoS threshold (initially 100 Gb/s) should be evaluated every \
 \ election cycle to see if it has to be raised due to newer \
 \ DDoS attack technologies."

scenario
  "DDOS_ATTACK_VALIDATION" -- @ref David Jefferson
description
  "The ability to survive a DDoS attack must be actually demonstrated \
 \ in the actual network configuration to be used prior to each \
```

```
 \ federal election."

scenario
  "DDOS_LOCAL_ELECTION" -- @ref David Jefferson
description
  "Reduced DDoS defense requirements might be acceptable for \
 \ non-federal elections."

end
```

1.18 SECURITY.BON

```
scenario_chart SECURITY_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS";
explanation
  "General security requirements for digital elections systems."

-- @ref Rec(2004)11 Security, I. General requirements
scenario "NO_DATA_LOSS" -- @ref Rec(2004)11 Appendix III, D. I. 77.
description
  "Technical and organizational measures shall be taken to ensure that \
 \ no data will be permanently lost in the event of a breakdown or a \
 \ fault affecting the e-voting system."

scenario "VOTER_PRIVACY_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. I. 78.
description
  "The e-voting system shall maintain the privacy of \
 \ individuals.  Confidentiality of voters' registers stored in or \
 \ communicated by the e-voting system shall be maintained."

scenario "SYSTEM_SELF_CHECKS" -- @ref Rec(2004)11 Appendix III, D. I. 79.
description
  "The e-voting system shall perform regular checks to ensure that its \
 \ components operate in accordance with its technical specifications \
 \ and that its services are available."

scenario "SYSTEM_ACCESS_CONTROL" -- @ref Rec(2004)11 Appendix III, D. I. 80.
description
  "The e-voting system shall restrict access to its services, \
 \ depending on the user identity or the user role, to those services \
 \ explicitly assigned to this user or role.  User authentication shall \
 \ be effective before any action can be carried out."

scenario "DATA_PROTECTION" -- @ref Rec(2004)11 Appendix III, D. I. 81.
description
  "The e-voting system shall protect authentication data so that \
 \ unauthorized entities cannot misuse, intercept, modify, or otherwise \
 \ gain knowledge of any of this data.  In uncontrolled \
 \ environments, authentication based on cryptographic mechanisms is \
 \ advisable."

scenario "UNIQUE_IDENTIFICATION" -- @ref Rec(2004)11 Appendix III, D. I. 82.
description
  "Identification of voters and candidates in a way that they can \
 \ unmistakably be distinguished from other persons (unique \
```

```
 \ identification) shall be ensured."

scenario "OBSERVATION_DATA" -- @ref Rec(2004)11 Appendix III, D. I. 83.
description
  "E-voting systems shall generate reliable and sufficiently detailed \
 \ observation data so that election observation can be carried \
 \ out.  The time at which an event generated observation data shall be \
 \ reliably determinable.  The authenticity, availability and \
 \ integrity of the data shall be maintained."

scenario "TIME_SYNCHRONIZATION" -- @ref Rec(2004)11 Appendix III, D. I. 84.
description
  "The e-voting system shall maintain reliable synchronized time \
 \ sources.  The accuracy of the time sources shall be sufficient to \
 \ maintain time marks for audit trails and observations data, as well \
 \ as for maintaining the time limits for registration, nomination, \
 \ voting, or counting."

scenario "SECURITY_COMPLIANCE_RESPONSIBILITY" -- @ref Rec(2004)11 Appendix III, D. I. 85.
description
  "The electoral authority has overall responsibility for compliance \
 \ with these security requirements, and such compliance shall be assessed by \
 \ independent bodies."

-- @ref Rec(2004)11 Security, II. Requirements in pre-voting stages
scenario "LISTS_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. II. 86.
description
  "The authenticity, availability and integrity of the voters' \
 \ registers and lists of candidates shall be maintained.  The source of \
 \ the data shall be authenticated.  Provisions on data protection shall \
 \ be respected."

scenario "CANDIDATE_PROCESS_TIME_PROVENANCE" -- @ref Rec(2004)11 Appendix III, D. II. 87.
description
  "The fact that candidate nomination and, if required, the decision \
 \ of the candidate and/or the electoral authority to accept a \
 \ nomination has happened within the prescribed time limits shall be \
 \ ascertainable."

scenario "VOTER_PROCESS_TIME_PROVENANCE" -- @ref Rec(2004)11 Appendix III, D. II. 88.
description
  "The fact that voter registration has happened within the prescribed \
 \ time limits shall be ascertainable."

-- @ref Rec(2004)11 Security, III. Requirements in the voting stage
scenario "ELECTION_DATA_INTEGRITY_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. III. 89.
description
  "The integrity of data communicated from the pre-voting stage \
 \ (e.g., voters' registers and lists of candidates) shall be \
 \ maintained.  Data-origin authentication shall be carried out."

scenario "BALLOT_AUTHENTICITY_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. III. 90.
description
  "It shall be ensured that the e-voting system presents an authentic \
 \ ballot to the voter.  In the case of remote e-voting, the voter shall \
 \ be informed about the means to verify that a connection to the \
 \ official server has been established and that the authentic ballot \
 \ has been presented."
```

```
scenario "CAST_VOTE_TIME_PROVENANCE" -- @ref Rec(2004)11 Appendix III, D. III. 91.
description
  "The fact that a vote has been cast within the prescribed time \
 \ limits shall be ascertainable."

scenario "CONTROLLED_SYSTEMS_AND_VOTE_INTEGRITY" -- @design derived from Rec(2004)11 Appendix III, D. III. 92.
description
  "Election equipment under the control of the electoral authority \
 \ shall be protected against influence that could modify the vote."

scenario "UNCONTROLLED_SYSTEMS_AND_VOTE_INTEGRITY" -- @ref Kiniry/Zimmerman
description
  "The integrity of the vote must not depend on the security of election \
 \ equipment not under the control of the electoral authority."

scenario "NO_BREADCRUMBS" -- @ref Rec(2004)11 Appendix III, D. III. 93.
description
  "Residual information holding the voter's decision or the display of \
 \ the voter's choice shall be destroyed after the vote has been \
 \ cast.  In the case of remote e-voting, the voter shall be provided \
 \ with information on how to delete, where that is possible, traces \
 \ of the vote from the device used to cast the vote."

scenario "ELIGIBILITY_IMPLIES_VOTE_VOTER_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. III. 94.
description
  "The e-voting system shall at first ensure that a user who tries to \
 \ vote is eligible to vote.  The e-voting system shall authenticate \
 \ the voter and shall ensure that only the appropriate number of votes \
 \ per voter is cast and stored in the electronic ballot box."

scenario "VOTE_CHOICE_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. III. 95.
description
  "The e-voting system shall ensure that the voter's choice is \
 \ accurately represented in the vote and that the sealed vote enters \
 \ the electronic ballot box."

scenario "END_OF_VOTE_PERIOD_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. III. 96.
description
  "After the end of the e-voting period, no voter shall be allowed to \
 \ gain access to the e-voting system.  However, the acceptance of \
 \ electronic votes into the electronic ballot box shall remain open \
 \ for a sufficient period of time to allow for any delays in the \
 \ passing of messages over the e-voting channel."

-- @ref Rec(2004)11 Security, IV. Requirements in post-voting stages
scenario "DATA_COMMUNICATION_INTEGRITY_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. IV. 97.
description
  "The integrity of data communicated during the voting stage \
 \ (e.g. votes, voters' registers, lists of candidates) shall be \
 \ maintained.  Data-origin authentication shall be carried out."

scenario "TALLY_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. IV. 98.
description
  "The counting process shall accurately count the votes.  The counting \
 \ of votes shall be reproducible."

scenario "BALLOT_BOX_AND_TALLY_INVARIANTS" -- @ref Rec(2004)11 Appendix III, D. IV. 99.
description
  "The e-voting system shall maintain the availability and integrity \
```

```
 \ of the electronic ballot box and the output of the counting process \
 \ as long as required."

scenario "ADVERSARY_RESOURCES" -- @ref Kiniry/Zimmerman
description
  "The e-voting system shall be designed and tested with the assumption \
 \ that an adversary has a budget of $10 per voter per election, which they \
 \ can apply toward any critical subset of votes/voters of their choosing."
end

scenario_chart E2EVIV_SECURITY_REQUIREMENTS
indexing
  partof: "SECURITY_REQUIREMENTS";
  author: "David Jefferson <d_jefferson@yahoo.com>";
  created: "22 June 2014";
  reviewer: "Joe Kiniry <kiniry@galois.com>";
  reviewed: "16 July 2014"
explanation
  "General security requirements for end-to-end verifiable internet \
 \ election systems."

 -- These are requirements for embedding an E2EV system in an Internet
 -- voting environment.  They are over and above the requirements for
 -- the core E2EV itself.  We do not consider usability or accessibility
 -- requirements here.  Some of these requirements will make
 -- accessibility and usability more difficult to achieve.  Still, these
 -- are requirements, and if they cannot be met, or cannot be met
 -- simultaneously with usability and accessibility requirement, then we
 -- have to recommend not implementing an E2EV Internet voting system.

scenario
  "NATIONAL_SECURITY" -- @ref David Jefferson
description
  "If used in federal elections, an Internet voting system is also a \
 \ national security system, and thus must be subject to the highest \
 \ security requirements."

scenario
  "FEDERAL_REQUIREMENTS" -- @ref David Jefferson
description
  "Any Internet voting system used in a public primary or general \
 \ election in the U.S. for federal or state legislative, executive, \
 \ or judicial office, or recall election, or statewide initiative or \
 \ referendum, must meet all of the requirements in this document."

scenario
  "LOCAL_REQUIREMENTS" -- @ref David Jefferson
description
  "Reduced security requirements might be appropriate for county, \
 \ municipal, or other kinds of elections"

scenario
  "AUTOMATED_REGISTRATION_FRAUD" -- @ref David Jefferson
description
  "Automated registration fraud must not be possible."

scenario
  "CLIENT_SIDE_AUTHENTICITY" -- @ref David Jefferson
description
```

```
  "There must be a means by which any third party can determine if the \
 \ client-side software is genuine."

scenario
  "AUTHENTICATION_INDEPENDENCE" -- @ref David Jefferson
description
  "The security of authentication must not be affected by \
 \ any potential breach of any public or commercial databases."

scenario
  "ZERO_KNOWLEDGE_AUTHENTICATION" -- @ref David Jefferson
description
  "It should not be possible for an attacker to impersonate voters \
 \ even if the entire server database used for authentication is \
 \ compromised."

scenario
  "AUTHENTICATION_CREDENTIAL_REESTABLISHMENT" -- @ref David Jefferson
description
  "In some cases of security breach it must be possible to require all \
 \ voters in a jurisdiction to re-establish credentials."
end

scenario_chart PRIVACY_REQUIREMENTS
indexing
  partof: "SECURITY_REQUIREMENTS"
explanation
  "General privacy requirements for end-to-end verifiable internet \
 \ election systems."
-- violations of vote privacy are not generally detectable
-- violations of vote privacy are irreversible
-- violations of vote privacy enable vote coercion and vote selling
-- vote privacy cannot be verified by testing; it can only be
--   ascertained by expert analysis of architecture and code

scenario
  "E2E_VOTE_PRIVACY" -- @ref David Jefferson
description
  "Vote privacy must be preserved end-to-end insofar as mathematically \
 \ possible."

scenario
  "VOTE_PRIVACY_INVIOLATE" -- @ref David Jefferson
description
  "Vote privacy cannot be waived by voters."

scenario
  "MALWARE_PRESENCE" -- @ref David Jefferson
description
  "Vote privacy must not be violated even in the presence of arbitrary \
 \ malicious code on the client platform, including phony client \
 \ software, malicious client wrappers, MITM code between the user and \
 \ the E2EV interface, malicious browser plugins or scripts, \
 \ keyloggers, etc."
 -- This requirement will seriously complicate the user interface an
 -- usability of the system, but is absolutely essential.

scenario
  "REMOTE_MONITORING" -- @ref David Jefferson
```

```
description
  "Voting should not be permitted from client platforms known to have \
 \ remote monitoring software installed that could be used to monitor \
 \ or log voting activity and that cannot be turned off by the voter. \
 \ (All mobile platforms had, and probably still do have, such remote \
 \ monitoring software.)"

scenario
  "CLIENT_SIDE_CHANNELS" -- @ref David Jefferson
description
  "The client software of the voting system must not send data to any \
 \ IP address except those associated with the vote server and the \
 \ basic infrastructure servers of the Internet."

scenario
  "SOCIAL_MEDIA_SIDE_CHANNELS" -- @ref David Jefferson
description
  "The client should not provide any information to third parties, \
 \ e.g., Facebook, Twitter, etc. regarding the act of voting."

scenario
  "NO_TRACKING" -- @ref David Jefferson
description
  "There must be no tracking devices or tracking logic in the vote \
 \ client."

scenario
  "NO_BREADCRUMBS_DETAILS" -- @ref David Jefferson
description
  "The client software must leave no files or other persistent data on \
 \ the platform regarding the vote transaction but for an optional \
 \ file containing information needed for subsequent verification that \
 \ the voter's ballot is included in the election canvass: no cookies \
 \ or other session files, no temporary files."

scenario
  "TRANSIENT_DATA_CLEANUP" -- @ref David Jefferson
description
  "The client software should explicitly erase (i.e., overwrite) all \
 \ transient copies of vote-transaction data, e.g. data in registers, \
 \ caches, RAM, and virtual memory."

scenario
  "FORENSICALLY_SECURE" -- @ref David Jefferson
description
  "It should not be possible even for client-side forensic tools to \
 \ retrieve any information regarding the voting transaction after the \
 \ voting session is ended."

scenario
  "REMOTE_ADMINISTRATION_FORBIDDEN" -- @ref David Jefferson
description
  "The voting system should not support platforms that have remote \
 \ administration or remote control tools installed that cannot be \
 \ turned off by the voter."

scenario
  "INVULNERABLE_TO_ELECTION_MALWARE" -- @ref David Jefferson
description
```

```
  "The voting system must not be vulnerable to malware designed to \
 \ modify votes before they are input to the E2EV system."
 -- This will seriously complicate the human interface and usability
 -- of the voting system, but is absolutely essential.  Malware can be
 -- in many forms: completely phony or "alternative" client app,
 -- client wrapper, client-side MITM, browser plugin, client APT, etc.

scenario
  "CLIENT_SYSTEM_AUTHENTICATION" -- @ref David Jefferson
description
  "The voting system server must authenticate that it is communicating \
 \ with a genuine vote client during a voting session."
 -- This will complicate, but not eliminate, the possibility of
 -- client-side malware.  @see CLIENT_SIDE_AUTHENTICITY.

scenario
  "PENETRATION_ATTACKS" -- @ref David Jefferson
description
  "The voting system must be resistant to penetration attacks."

scenario
  "APT_ATTACKS" -- @ref David Jefferson
description
  "The voting system must be resistant to advanced persistent \
 \ threat attacks."

scenario
  "INSIDER_ATTACKS" -- @ref David Jefferson
description
  "It should not be possible for an insider to attack the voting \
 \ system without being detected."

scenario
  "COERCION_PREVENTION" -- @ref David Jefferson
description
  "There must be no way for voters to prove to another party any \
 \ information regarding how they voted in any race beyond what is \
 \ mathematically deducible from the final distribution of votes."
  -- @see RECEIPT_FREEDOM

scenario
  "STRONG_SOFTWARE_INDEPENDENCE" -- @ref Ron Rivest
description
  "The system must witness strong software independence: an \
 \ undetected change or error in its software cannot cause an
 \ undetectable change or error in an election outcome, and \
 \ moreover, a detected change or error in an election outcome \
 \ (due to change or error in the software) can be corrected \
 \ without re-running the election."

scenario
  "DIGITAL_EVIDENCE_NOT_A_RECEIPT"
description
  "Digital evidence (e.g., photographing a ballot or video recording \
 \ the casting process) of the voting process must not violate receipt \
 \ freedom."
end

scenario_chart CERTIFICATION_AND_RECERTIFICATION_REQUIREMENTS
```

```
indexing
  partof: "SECURITY_REQUIREMENTS"
explanation
  "General security requirements relating to certification of digital \
 \ elections systems."
end
```

1.19 USABILITY.BON

```
scenario_chart USABILITY_REQUIREMENTS
indexing
  partof: "TECHNICAL_REQUIREMENTS"
explanation
  "General usability requirements of digital elections systems."

scenario
  "MANDATORY_USABILITY_TESTING" -- @ref Kiniry/Zimmerman
description
  "Usability testing for disabled and abled voters shall be performed, \
 \ and the reports of the testing made public. The system must achieve \
 \ satisfactory usability testing results before being used in a \
 \ binding election."

scenario
  "VOTE_CONFIRMATION" -- @ref David Jefferson
description
  "If a voter receives the final ‘Thank you for voting’ confirmation, \
 \ then she/he can be certain the ballot was recorded."

scenario
  "UNCERTAIN_VOTER_REVOTE" -- @ref David Jefferson
description
  "If the voter is uncertain about the state of their ballot, he/she \
 \ is free to attempt to vote again."

end
```

CHAPTER 2

BON REPRESENTATION OF E2E-VIV DOMAIN MODEL

The following is a comprehensive domain model for an E2E-VIV system, in the form of a BON specification. The corresponding BON file is available in the E2E-VIV GitHub repository, at https://github.com/GaloisInc/e2eviv.

2.1 E2EVIV.BON

```
-- This E2E VIV specification is written in the EBON specification
-- language, based upon the BON specification language from Walden and
-- Nerson.  See http://bon-method.com/ for more information about BON
-- and http://kindsoftware.com/ for more information about EBON.  Tool
-- support for EBON is provided by the BON compiler, bonc, and several
-- other tools.  See https://github.com/kiniry/BON for more
-- information.

-- Informal Charts

-- BON Domain Model

system_chart E2EVIV_SYSTEM
indexing
  author: "Joseph Kiniry <kiniry@galois.com>", "Daniel M. Zimmerman <dmz@galois.com>";
  organization: "Galois, Inc.";
  keywords: "OVF", "end-to-end verifiable internet voting", "e2e", "viv",
    "verifiable elections", "software independence",
    "high-assurance", "cryptography", "verification", "Galois";
  created: "Tue Jul 15 16:18:09 PDT 2014";
  revised: "February 2015";
  github: "https://github.com/GaloisInc/e2eviv";
explanation
  "An end-to-end verifiable Internet voting system"
cluster CORE_CONCEPTS
description
  "Core concepts generic to all elections."
cluster LEGAL_STANDARDS
description
```

```
  "Basic legal standards generic to democratic elections."
cluster PERSONAS
description
  "Archetypical personas for actors participating in elections."
end

cluster_chart CORE_CONCEPTS
explanation
  "Domain concepts core to the idea of elections."
cluster ACTIONS
description "State transitions that take place in the course of an election."
cluster BACKGROUND
description "Election background concepts."
cluster ELECTION_DAY_ARTIFACTS
description "Artifacts relevant to election day."
cluster PEOPLE
description "People that are part of an electoral system."
cluster PROPERTIES
description "Properties of elections and their artifacts."
cluster OTHERS
description "Placeholder for concepts waiting to be clustered."
end

cluster_chart BACKGROUND
explanation
  "Background concepts relevant to elections in the general."
class CONTEST
  description "A decision to be made, either the selection of one or  \
              \ more candidates for an office or the choice of a course of \
              \ action."
class DEMOCRACY
  description "A system of government by an entire population or \
              \ eligible members thereof."
class ELECTION
  description "A formal process of selecting choices in one or more contests."
class ELECTORATE
  description "The individuals that are eligible to vote in an election."
class EVOTING
  description "A voting process carried out with the aid of electronic devices."
class INTERNET
  description "A global system of interconnected computer networks."
class PARTY
  description "An organized group of people with at least roughly similar \
              \ political aims."
class PRINCIPLE
  description "A fundamental truth or proposition that serves as a foundation \
              \ for a system of belief or behavior or chain of reasoning."
class PROCEDURE
  description "An established or official way of doing something."
class SYSTEM
  description "A set of connected digital and physical parts, including computers, \
              \ people, organizations, and more, forming a complex whole."
class VOTING_CHANNEL
  description "Methods by which voters are enabled to vote in elections."
cluster ELECTIONS
  description "Types and attributes of elections."
cluster PROCESSES
  description "A series of actions or steps taken in order to achieve a \
              \ particular end."
```

```
end

cluster_chart ELECTIONS
explanation
  "Types and attributes of elections."
class DIGITAL_ELECTION
  description "An election carried out, in whole or in part, \
              \ by electronic means."
class INTERNET_ELECTION
  description "An election carried out, in whole or in part, \
              \ using the Internet for the transmission of votes."
class SUPERVISED_ELECTION
  description "An election where election officials, and perhaps the public, \
              \ watch over the election, primarily to ensure that voters have \
              \ privacy when voting."
class REMOTE_ELECTION
  description "An election in which some or all of the ballots \
              \ are not cast at polling stations."
class TRADITIONAL_ELECTION
  description "An election carried out entirely using physical \
              \ ballots cast at polling stations during \
              \ a fixed election period."
class UNSUPERVISED_ELECTION
  description "An election where there are no observers ensuring voter \
              \ privacy."
class VERIFIABLE_ELECTION
  description "An election scheme whereby one or more formal \
              \ properties of the election can be independently checked \
              \ by voters or election officials."
end

cluster_chart ELECTION_DAY_ARTIFACTS
explanation
  "Physical and digital artifacts relevant to election day."
class BALLOT
  description "The legally recognized means by which a voter can \
              \ express his or her choices in one or more contests \
              \ in an election."
class BALLOT_BOX
  description "The means by which ballots are stored pending being \
              \ counted."
class BALLOT_CONFIGURATION
  description "The set of contests in which voters of a particular \
              \ group are eligible to vote."
class BALLOT_QUESTION
  description "A decision among two or more courses of action."
class BALLOT_STYLE
  description "The concrete presentation of a ballot configuration."
class CANDIDATES_REGISTER
  description "A listing of the candidates standing for election."
class CONTEST_CHOICE
  description "A selection from among the possible outcomes of \
              \ a contest."
class CONTEST_FOR_OFFICE
  description "A selection of some subset of candidates standing for \
              \ election to a particular office."
class RESULT
  description "The outcome of a contest."
class SEAL
```

```
  description "A device, algorithm, or process that provides evidence \
              \ for the integrity of an object."
class TALLY
  description "The count of all the votes in an election."
class VOTE
  description "The expression of a contest choice."
class VOTERS_REGISTER
  description "A listing of the eligible voters for an election."
class VOTING_INTERFACE
  description "The medium through which a voter makes his or \
              \ her contest choices known to the voting system."
cluster PHYSICAL_ARTIFACTS
  description "Physical artifacts relevant to election day."
cluster DIGITAL_ARTIFACTS
  description "Digital artifacts relevant to election day."
end

cluster_chart PHYSICAL_ARTIFACTS
explanation
  "Physical artifacts relevant to election day."
class DEVICE
  description "A physical artifact that is fit for a particular purpose."
class PHYSICAL_BALLOT_BOX
  description "A box used to store paper ballots pending being counted."
class PAPER_BALLOT
  description "A ballot comprised of one or more pieces of paper."
class POLLING_STATION
  description "A location at which physical ballot boxes and devices \
              \ are available for members of the electorate to use."
class PAPER_VOTE
  description "A vote expressed with a paper ballot."
class PHYSICAL_SEAL
  description "A piece of material that serves as evidence that \
              \ a physical artifact has not been tampered with."
end

cluster_chart DIGITAL_ARTIFACTS
explanation
  "Digital artifacts relevant to election day."
class DIGITAL_BALLOT
  description "A digital manifestation of a paper ballot record."
class DIGITAL_BALLOT_BOX
  description "The electronic means by which digital ballots are \
              \ stored pending being counted."
class DIGITAL_VOTE
  description "A vote expressed with a digital ballot."
class DIGITAL_SEAL
  description "A digital artifact that serves as evidence that \
              \ another digital artifact has not been tampered with."
end

cluster_chart PROPERTIES
explanation
  "Properties of elections and related artifacts."
class ACCESSIBLE
  description "Usable by and useful to the disabled."
class AUTHENTICATED
  description "A person or system that has properly identified itself."
class CONFIDENT
```

```
  description "A person or system that is certain about a proposition."
class DIGITAL
  description "An artifact that is manifested via information, rather than as \
              \ a tangible artifact."
class DISABLED
  description "Having a physical or mental condition \
              \ that limits movements, senses, or activities."
class EFFICIENT
  description "A system that operates in a productive fashion with \
              \ little wasted effort or expense."
class REMOTE
  description "Located somewhere other than a polling station."
class ROBUST
  description "A process or system that is able to withstand adverse \
              \ conditions."
class PHYSICAL
  description "Manifested as a tangible artifact."
class SUPERVISED
  description "A person or system that is directly observed."
class TURNOUT
  description "The level of participation of voters in an election."
class UNSUPERVISED
  description "A person or system that has no observers."
class VERIFIABLE
  description "A system or algorithm that has properties which can be \
              \ checked by people or digital systems."
cluster ELECTION_PROPERTIES
  description "Properties specific to elections."
cluster SYSTEM_PROPERTIES
  description "Properties specific to systems used to \
              \ carry out elections."
end

cluster_chart PROCESSES
class AUDIT
  description "A review of the election artifacts to detect \
              \ abnormalities and errors."
class CANDIDATE_REGISTRATION
  description "The process by which a candidate is added to \
              \ the candidates register."
class CANDIDATE_VALIDATION
  description "The process by which a candidate's identity and \
              \ eligibility to stand for election are verified."
class VOTER_REGISTRATION
  description "The process by which a member of the electorate is added \
              \ to the voter register."
class VOTER_VALIDATION
  description "The process by which a voter's identity and \
              \ eligibility to vote are verified."
class VERIFICATION
  description "A process by which the the election protocols, \
              \ processes, and device implementations are proven \
              \ to be correct with respect to their specifications."
end

cluster_chart ACTIONS
explanation
  "State transitions that take place in the course of an election."
class AUTHENTICATE
```

```
  description "Transitioning a person or system to an authenticated state."
class REGISTER_VOTER
  description "The addition of a voter to the voters register."
class REGISTER_CANDIDATE
  description "The addition of a candidate to the candidates register."
class UNREGISTER_VOTER
  description "The removal of a voter from the voters register."
class UNREGISTER_CANDIDATE
  description "The removal of a candidate from the candidates register."
end

cluster_chart ELECTION_PROPERTIES
explanation
  "Properties specific to elections."
class SECURITY
  description "The attestation that a system is free of certain classes of \
              \ dangers or threats."
cluster SCOPE
  description "The geographic or logical area affected by an election."
end

cluster_chart SCOPE
explanation
  "The geographic or logical area affected by an election."
class INTERNATIONAL
  description "A scope comprised of multiple nations."
class LOCAL
  description "A scope comprised of a single locality or \
              \ small group of localities."
class NATIONAL
  description "A scope comprised of a single nation."
class REGIONAL
  description "A scope comprised of a large group of localities \
              \ or a single state, territory, or similar region"
end

cluster_chart SYSTEM_PROPERTIES
explanation
  "Properties held by election systems, digital or physical."
class ACCESSIBLE
  description "An artifact is accessible if it is usable and useful to \
              \ the disabled."
class RELIABLE
  description "An artifact is reliable if it is guaranteed to be \
              \ available for use, and to work properly, for a \
              \ specified percentage of time."
class USABLE
  description "An artifact is usable if it can successfully be \
              \ used for its stated purpose."
end

cluster_chart PEOPLE
explanation
  "The people that are part of an electoral system.  These are the most \
 \ general concepts explaining roles in an election from a legal standpoint. \
 \ Personas, as specified in the PERSONAS cluster, further concretize these \
 \ general classes into specific UX-centric roles."
class CANDIDATE
  description "A citizen who is standing for election."
```

```
class CITIZEN
  description "A person who legally belongs to a place and \
              \ has the rights and protections of that place."
class ELECTORAL_AUTHORITY
  description "An individual or group responsible for setting up, \
              \ running, and disclosing the results of an election."
class IDENTITY
  description "The fact of being who or what a person or system is."
class PERSON
  description "An individual."
class VOTER
  description "A person who is eligible to vote in an election."
end

cluster_chart LEGAL_STANDARDS
explanation
  "Basic legal standards generic to democratic elections."
class LEGISLATION
  description "A set of laws."
end

class_chart ACCESSIBLE
indexing
  applicable_law: "http://www.section508.gov"
explanation
  "An artifact is accessible if it is usable by and useful to the \
 \ disabled.  The details of such a notion are often codified in \
 \ federal law (e.g., U.S. Section 508) and are the results of \
 \ researchers focused on user experiences for the disabled."
end

class_chart AUDIT
explanation
  "An audit is a review of the election artifacts to detect \
 \ abnormalities and errors."
query
  "Were any errors detected?"
end

class_chart AUTHENTICATE
explanation
  "A person or system that has properly identified itself."
end

class_chart BALLOT
explanation
  "A ballot is the legally recognized means by which a voter \
 \ can express his or her choices for one or more contests in an \
 \ election. A ballot contains a set of votes corresponding to \
 \ the contests being decided in the election."
query
  "What is your ballot style?",
  "Have you been cast?",
  "Have you been spoiled?",
  "What votes do you contain?",
  "What vote do you contain for the_contest?"
command
  "Your ballot style is the_style!",
  "You are cast!",
```

```
  "You are spoiled!",
  "You contain the_vote for the_contest!",
  "You no longer contain a vote for the_contest!"
constraint
  "Initially a ballot is not cast, not spoiled, and contains no votes.",
  "A ballot's style may only be set once.",
  "Once a ballot is cast or spoiled, the set of votes it contains \
 \ cannot be changed.",
  "Once a ballot is cast, it remains cast forever.",
  "Once a ballot is spoiled, it remains spoiled forever.",
  "A ballot cannot be both cast and spoiled.",
  "A ballot may contain at most one vote per contest.",
  "A ballot may only contain votes for contests that are part of its \
 \ ballot style."
end

class_chart BALLOT_BOX
explanation
  "A ballot box is the means by which ballots are stored pending \
 \ being counted. It may take various forms, including physical \
 \ containers (from which the name derives) and electronic \
 \ storage media."
query
  "Are you empty?",
  "Are you full?",
  "What is your capacity?",
  "How many ballots do you contain?",
  "What ballots do you contain?",
  "What seals are applied to you?",
  "Are you sealed?"
command
  "You contain the_ballot!",
  "You no longer contain the_ballot!",
  "The_seal is applied to you!",
constraint
  "A ballot box is initially empty and has no seals.",
  "Only cast ballots may be added to a ballot box.",
  "Ballots that are not in a ballot box cannot be \
 \ removed from the ballot box.",
  "A ballot box is sealed if and only if it has one or \
 \ more unbroken seals applied to it.",
  "Ballots may not be added to a full or sealed ballot box.",
  "Ballots may not be removed from an empty or sealed ballot box.",
  "A ballot box's capacity is non-negative.",
  "A ballot box is full if and only if it contains a number of \
 \ ballots equal to its capacity."
end

class_chart BALLOT_CONFIGURATION
explanation
  "A ballot configuration is the set of contests in which voters \
 \ of a particular group are eligible to vote."
query
  "What contests do you contain?",
  "Are you locked?"
command
  "You contain the_contest!",
  "You do not contain the_contest!",
  "You are locked!"
```

```
constraint
  "A ballot configuration is initially unlocked and contains \
 \ no contests.",
  "A contest may not be added to a ballot configuration more \
 \ than once.",
  "Ballot configurations that contain no contests may not be \
 \ locked.",
  "A contest may not be added to or removed from a locked \
 \ ballot configuration.",
  "Once locked, a ballot configuration remains locked forever."
end

class_chart BALLOT_QUESTION
explanation
  "A ballot question is a decision among two or more courses of \
 \ action. In most cases, ballot questions take the form of yes/no \
 \ questions."
inherit CONTEST
constraint
  "The maximum number of choices that may be chosen on the same \
 \ ballot is 1.",
  "Each choice represents a course of action."
end

class_chart BALLOT_STYLE
explanation
  "A ballot style is the concrete presentation of a ballot \
 \ configuration. A single ballot configuration may be realized \
 \ by several ballot styles, e.g. for different languages or \
 \ different orderings of contests or contest choices."
query
  "What is your ballot configuration?",
  "What are the details of your presentation?" -- highly implementation dependent
command
  "Your ballot configuration is the_configuration!"
constraint
  "A ballot style's ballot configuration may only be set once.",
  "A ballot style's ballot configuration may only be set to a \
 \ locked ballot configuration."
end

class_chart CANDIDATE
explanation
  "A candidate is a citizen who is listed on the ballot as a \
 \ possible choice to fill some position."
inherit CITIZEN
-- constraint
 -- various constraints apply to candidates for various offices,
 -- depending on the office (e.g., >= 35 yrs old, permanent
 -- resident in the U.S. for >= 14 yrs, and born a U.S.
 -- citizen are constraints on candidates for President of the
 -- United States).
end

class_chart CANDIDATES_REGISTER
explanation
  "A candidates' register contains all the candidates standing \
 \ for election and the offices for which they are standing."
query
```

```
  "Do you contain the_candidate?",
  "What candidates do you contain?",
  "Are you locked?"
command
  "You contain the_candidate!",
  "You do not contain the_candidate!",
  "You are locked!"
constraint
  "A register is initially empty and unlocked.",
  "A candidate may not be added to the register more than once.",
  "A candidate who is not in the register cannot be removed from \
 \ the register.",
  "Candidates may not be added to or removed from a locked register.",
  "A locked register may not be unlocked.",
  "A candidate added to the register must be alive at the time of \
 \ addition."
end

class_chart CITIZEN
explanation
  "A citizen is a person who legally belongs to a place and \
 \ has the rights and protections of that place. The place can \
 \ be at any election scope; for example, a particular person \
 \ may be a citizen of the United States, of Oregon, and of \
 \ Portland simultaneously."
inherit PERSON
query
  "What is your current residence address?",
  "What is your citizenship information?"
command
  "Your current residence address is the_address!",
  "Your citizenship information is the_information!"
end

class_chart CONFIDENT
explanation
  "A person or system that is certain about a proposition."
end

class_chart CONTEST
explanation
  "A contest is a decision to be made, either the selection of one or  \
 \ more candidates for an office or the choice of a course of action. \
 \ There may be multiple contests in a single election."
query
  "What are your contest choices?",
  "Do you allow a write-in choice?",
  "What is the maximum number of your contest choices that can be chosen \
 \ on the same ballot?",
  "What is your result?",
  "Does the_vote contain valid choices for you?"
command
  "Your contest choices are the_choices!",
  "You do/do not allow a write-in choice!",
  "Your result is the_result!",
  "The_maximum_number of your contest choices can be chosen on the \
 \ same ballot!"
constraint
  "A contest must have at least one contest choice.",
```

```
  "The result must contain information about every contest choice \
 \ in the contest.",
  "The contest choices for a contest may only be set once.",
  "The write-in allowed flag may only be set once.",
  "The result for a contest may only be set once.",
  "The maximum number of contest choices that can be chosen on the same \
 \ ballot may only be set once."
end

class_chart CONTEST_CHOICE
explanation
  "A selection from among the possible outcomes of a contest."
end

class_chart CONTEST_FOR_OFFICE
explanation
  "A contest for office is a selection of some subset of candidates \
 \ standing for election to a particular office."
inherit CONTEST
constraint
  "The contest choices represent individual candidates for an office."
end

class_chart DEMOCRACY
explanation
  "Democracy is a system of government (of a nation, \
 \ state, locality, or other organization) by an entire \
 \ population or eligible members thereof, typically \
 \ carried out through elections of leaders and \
 \ representatives, through referenda, or both."
end

class_chart DEVICE
explanation
  "A physical artifact that is fit for a particular purpose."
end

class_chart DIGITAL_BALLOT
explanation
  "A digital ballot is a ballot comprised of one or more \
 \ digital artifacts."
inherit BALLOT
end

class_chart DIGITAL_BALLOT_BOX
explanation
  "A digital ballot box is the electronic means by which \
 \ digital ballots are stored pending being counted."
inherit BALLOT_BOX
end

class_chart DIGITAL_SEAL
explanation
  "A digital seal is a piece of evidence that a digital \
 \ artifact has not been tampered with. Such seals \
 \ typically take the form of cryptographic hashes."
inherit SEAL
end
```

```
class_chart DISABLED
explanation
  "An individual is disabled if he or she has a physical or \
 \ mental condition that limits movements, senses, or \
 \ activities in a way that affects his or her ability to \
 \ participate in an election."
end

class_chart EFFICIENT
explanation
  "A system that operates in a productive fashion with little wasted \
 \ effort or expense."
end

class_chart ELECTION
explanation
  "An election is a formal indication of choices \
 \ in one or more contests."
end

class_chart ELECTORAL_AUTHORITY
explanation
  "An electoral authority is an individual or group responsible \
 \ for setting up, running, and disclosing the results of an election."
query
  "Who are your members?"
command
  "The_citizen is one of your members!",
  "The_citizen is not one of your members!"
constraint
  "An electoral authority must have at least one member."
end

class_chart ELECTORATE
explanation
  "The electorate for a given election comprises all the \
 \ individuals that are eligible to vote in that election, \
 \ according to applicable laws and regulations."
end

class_chart EVOTING
explanation
  "E-Voting, or electronic voting, is the process of voting either \
 \ entirely using, or with substantial assistance from, electronic \
 \ devices."
end

class_chart IDENTITY
explanation
  "The fact of being who or what a person or system is."
end

class_chart INTERNATIONAL
explanation
  "An international scope is comprised of multiple nations; \
 \ for example, the European Union."
end

class_chart INTERNET
```

```
explanation
  "The Internet is a global system of interconnected computer \
 \ networks that use the standard Internet Protocol suite to \
 \ link billions of connected devices."
end

class_chart LEGISLATION
explanation
  "Legislation is a set of laws. In this context, it is \
 \ the set of laws dealing with the conduct of elections."
end

class_chart LOCAL
explanation
  "A local scope is comprised of a single locality or a small \
 \ group of localities. Examples include individual towns and counties."
end

class_chart NATIONAL
explanation
  "A national scope is comprised of a single nation."
end

class_chart PAPER_BALLOT
explanation
  "A paper ballot is a ballot implemented using paper, which \
 \ a voter marks in some fashion to indicate his or her choice."
inherit BALLOT
end

class_chart PAPER_VOTE
explanation
  "A paper vote is a vote expressed with a paper ballot."
inherit VOTE
-- queries, commands, constraints to do with legibility and
-- interpretation of voter intent?
end

class_chart PERSON
explanation
  "A person is an individual with a unique identity."
query
  "What is your name?",
  "What is your date of birth?",
  "Are you alive?"
command
  "Your name is the_name!",
  "Your date of birth is the_date!",
  "You are not alive!"
constraint
  "A person is initially alive.",
  "A person's date of birth may only be set once.",
  "A person's date of birth must be in the past.",
  "Once a person is not alive, he stays not alive forever."
end

class_chart PARTY
explanation
  "A party is an organized group of people having at least roughly \
```

```
 \ similar political aims and opinions, that seeks to influence \
 \ public policy by getting its candidates elected to public office."
end

class_chart PHYSICAL_BALLOT_BOX
explanation
  "A physical ballot box is a box used to store paper ballots \
 \ pending being counted."
inherit BALLOT_BOX
query
  "What is your chain of custody?"
command
  "Add the_entry to your chain of custody!"
constraint
  "The capacity of a physical ballot box is finite.",
  "A physical ballot box may only be sealed with physical seals.",
  "A physical ballot box may only contain paper ballots.",
  "Entries may not be removed from the chain of custody.",
  "Each entry added to the chain of custody must represent one or \
 \ more individuals."
end

class_chart PHYSICAL_SEAL
explanation
  "A physical seal is a piece of material (such as tape) that \
 \ serves as evidence that a physical artifact has not been \
 \ tampered with. Such a seal typically has a distinctive design \
 \ and other features that make it obvious when a sealed artifact \
 \ has been tampered with."
inherit SEAL
query
  "What is your identifier?"
command
  "Your identifier is the_identifier!"
constraint
  "The identifier of a physical seal may only be set once."
end

class_chart POLLING_STATION
explanation
  "A polling station is a location at which physical ballot \
 \ boxes and devices are available for members of the \
 \ electorate to use during an election. Polling stations \
 \ are typically staffed by poll workers and have well-publicized \
 \ hours of operation."
end

class_chart PRINCIPLE
explanation
  "A principle is a fundamental truth or proposition that serves \
 \ as a foundation for a system of belief or behavior or chain \
 \ of reasoning."
end

class_chart PROCEDURE
explanation
  "A procedure is an established or official way of doing something."
end
```

```
class_chart REGIONAL
explanation
  "A regional scope is comprised of a large group of localities \
 \ or a single state, territory, or similar region. For example, \
 \ the state of California."
end

class_chart RELIABLE
explanation
  "An artifact is reliable if it is guaranteed to be \
 \ available for use, and to work properly, for a \
 \ specified percentage of time."
query
  "What is your reliability percentage?"
constraint
  "The reliability percentage must be between 0 and 100, \
 \ inclusive"
end

class_chart REMOTE
explanation
  "Something is remote if it is located somewhere other \
 \ than a polling station."
end

class_chart RESULT
explanation
  "A result is the outcome of a contest."
query
  "What contest choices do you contain counts for?",
  "What is the count for the_choice?"
command
  "The count for the_choice is the_number_of_votes!"
constraint
  "The count for each contest choice may only be set once."
end

class_chart ROBUST
explanation
  "A process or system is robust if it is able to \
 \ withstand adverse conditions."
end

class_chart SEAL
explanation
  "A seal provides some evidence of the integrity of another \
 \ entity (such as a ballot or ballot box). Its form depends on \
 \ the form of the entity being sealed, as well as other system \
 \ characteristics."
query
  "Are you applied?",
  "What are you applied to?",
  "Are you broken?"
command
  "You are applied to the_entity!",
  "Break!"
constraint
  "A seal is initially not applied and not broken.",
  "A seal may only be applied if it has not previously been applied \
```

```
 \ or broken.",
  "A seal may only be broken if it has not previously been broken.",
  "Once applied, a seal remains applied forever.",
  "Once broken, a seal remains broken forever."
end

class_chart SECURITY
explanation
  "Security is the attestation that a system is free of certain \
 \ classes of dangers or threats."
end

class_chart SYSTEM
explanation
  "A system is a set of connected digital and physical parts, \
 \ including computers, people, organizations, and more, \
 \ forming a complex whole."
end

class_chart TALLY
explanation
  "The tally is the count of all the votes in an election."
end

class_chart TURNOUT
explanation
  "Turnout is the level of participation of voters in a contest."
end

class_chart USABLE
explanation
  "An artifact is usable if it can successfully be used for its stated \
 \ purpose."
end

class_chart VERIFIABLE
explanation
  "A system or algorithm is verifiable if it has properties \
 \ that can be checked by people or digital systems."
end

class_chart VERIFICATION
explanation
  "Verification is a process by which the the election \
 \ protocols, processes, and device implementations are proven \
 \ to be correct with respect to their specifications."
end

class_chart VOTE
explanation
  "A vote is an expression of a contest choice made by a voter \
 \ during an election."
query
  "What contest choice do you represent?"
command
  "You represent the_choice!"
constraint
  "The choice represented by a vote may only be set once."
end
```

```
class_chart VOTER
explanation
  "A voter is a person who is eligible to vote in an election. \
 \ A voter has affiliations with various groups (districts, \
 \ political parties, etc.) that determine the voter's \
 \ eligibility to vote in specific contests."
inherit CITIZEN
query
  "What groups are you in?"
command
  "You are in the_group!",
  "You are not in the_group!"
end

class_chart VOTER_REGISTRATION
explanation
  "Voter registration is the process by which a member of \
 \ the electorate is added to the voters' register."
end

class_chart VOTERS_REGISTER
explanation
  "A voters' register contains all the voters eligible \
 \ to vote in an election, as well as information \
 \ indicating the ballot configuration each voter should \
 \ use and whether each has participated in the election."
query
  "Is the_voter in the register?",
  "What ballot configuration should be used with the_voter?",
  "Has the_voter voted?"
command
  "Add the_voter to the register!",
  "Remove the_voter from the register!",
  "Set the_voter's ballot configuration to the_configuration!",
  "the_voter has voted!"
constraint
  "A voter may not be added to the register more than once.",
  "A voter may not be removed from the register if he has voted.",
  "Once a voter is marked as having voted, he remains so marked forever.",
  "Once a voter is marked as having voted, his ballot configuration may \
 \ not change."
end

class_chart VOTING_CHANNEL
explanation
  "A voting channel is a method by which voters are enabled \
 \ to vote in elections."
end

class_chart VOTING_INTERFACE
explanation
  "A voting interface is the medium through which a voter \
 \ makes his or her contest choices known to the voting system."
end
```