**GENERAL\_MTBF**

The entire voting service (server side) must have a proven MTBF of >168 hours (1 week) under peak expected voting loads the entire time.

**LIVE\_ELECTION\_MTBF**

MTBF validation must be demonstrated in multiple tests of actual mock elections.

**MTBF\_CONTRA\_DDOS**

MTBF requirements apply only during normal peak operation, not during attacks (e.g., DDoS).

**SYSTEM\_RECOVERY\_TIME**

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.

**UPTIME**

The system must have three nines (99.9%) uptime.

**FAILURE\_VALIDATION**

Uptime must be demonstrated by failures in actual mock election situations, e.g. tested by sudden loss of power to any server.

**MIRRORED\_FAILOVER\_SERVICE**

The system must have a warm spare in a second data center that can take over in case of major failure.

**FAILOVER\_STAFFING**

The system must be staffed at all times to guarantee the 10 minute recovery time.

**OPERATION\_UNDER\_DDOS**

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.

**DDOS\_REFRESH\_PERIODICITY**

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.

**DDOS\_ATTACK\_VALIDATION**

The ability to survive a DDoS attack must be actually demonstrated in the actual network configuration to be used prior to each federal election.

**DDOS\_LOCAL\_ELECTION**

Reduced DDoS defense requirements might be acceptable for non-federal elections.

**MAINTENANCE\_REQUIREMENTS**

**ELECTORAL\_AUTHORITY\_PATCH**

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

**EVOLVABILITY\_REQUIREMENTS**

**ELECTORAL\_AUTHORITY\_UPDATE**

The electoral authority has the right and ability to update election systems to conform to changes in applicable law, available technology, or the system threat model.

**MANDATORY\_ACCESSIBILITY\_TESTING**

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.

**UNIVERSAL\_ACCESSIBILITY**

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.

**ACCESSIBILITY\_STAKEHOLDERS**

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.

**USER\_FACILITIES\_FOR\_ACCESSIBILITY**

Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance.

**COMPLEMENT\_ACCESSIBILITY\_TECHNOLOGIES**

Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.

**ACCESSIBLE\_VOTING\_OPTIONS**

The presentation of the voting options shall be optimized for the voter.

**CASTING\_ATOMIC**

Ballot casting shall be atomic with respect to server failures.

**DETERMINISTIC\_VOTING\_PROCESS**

If a server side failure occurs, no voter's balloting can be left in an unknown state.

**BALLOT\_FINAL\_STATES**

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.

**VOTE\_RECORD\_MONOTONICITY**

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.

**RECEIPT\_FREEDOM**

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).

**VALID\_BALLOT\_PROVENANCE**

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.

**MULTI\_BALLOT\_RECORD**

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.

**NO\_DOUBLE\_VOTE**

But for systems supporting MULTI\_BALLOT\_RECORD, the voting system shall not record more than one vote for any voter in any race.

**NO\_ADVERTISING**

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.

**NO\_EXTERNAL\_LINKS**

The voting system client must not display any links to other sites except for help in the mechanics of voting.

**INTEROPERABILITY\_REQUIREMENTS**

**OPEN\_STANDARDS**

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.

**EML**

The Election Markup Language (EML) shall be used whenever possible for e-election and e-referendum applications.

**DATA\_LOCALIZATION**

In cases that imply specific election or referendum data requirements, a localization procedure shall be used to accommodate these needs.

**OPEN\_LOG\_FORMATS**

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.

**USABLE\_UI**

The voter interface of an e-voting system shall be understandable and easily usable.

**UNIMPEDED\_REGISTRATION**

Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.

**MAXIMIZE\_DISABLED\_ACCESSIBILITY**

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.

**REMOTE\_ONLY\_SUPPLEMENTARY**

Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

**AT\_MOST\_ONE\_VOTE\_PER\_VOTER**

The e-voting system shall ensure that at most one electronic vote from each voter is included in the final tally.

**VALID\_TALLY**

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.

**VOTE\_AGGREGATION**

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.

**FREE\_SUFFRAGE**

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.

**REFLECTIVE\_VOTING\_PROCESS**

The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.

**FLEXIBLE\_VOTING\_PROCESS**

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.

**NO\_VOTER\_MANIPULATION**

The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.

**BLANK\_VOTE**

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.

**CONCLUSION\_OF\_VOTING\_PROCESS**

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.

**IMMUTABLE\_VOTES**

Except in systems supporting MULTI\_BALLOT\_RECORD, the e-voting system shall prevent the changing of a vote once that vote has been cast.

**SECRET\_SUFFRAGE**

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.

**ANONYMOUS\_VOTES**

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.

**NO\_INDIRECT\_SECRECY\_VIOLATION**

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.

**NO\_SECRET\_SUFFRAGE\_SIDE\_CHANNEL**

Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

**NO\_NDAS\_FOR\_STUDY**

No nondisclosure agreement or any other contract shall be required to download and study the Internet voting system.

**NO\_NDAS\_FOR\_AUDIT**

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.

**NO\_DATA\_LOSS**

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.

**VOTER\_PRIVACY\_INVARIANTS**

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.

**SYSTEM\_SELF\_CHECKS**

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.

**SYSTEM\_ACCESS\_CONTROL**

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.

**DATA\_PROTECTION**

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.

**UNIQUE\_IDENTIFICATION**

Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.

**OBSERVATION\_DATA**

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.

**TIME\_SYNCHRONIZATION**

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.

**SECURITY\_COMPLIANCE\_RESPONSIBILITY**

The electoral authority has overall responsibility for compliance with these security requirements, and such compliance shall be assessed by independent bodies.

**LISTS\_INVARIANTS**

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.

**CANDIDATE\_PROCESS\_TIME\_PROVENANCE**

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.

**VOTER\_PROCESS\_TIME\_PROVENANCE**

The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

**ELECTION\_DATA\_INTEGRITY\_INVARIANTS**

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.

**BALLOT\_AUTHENTICITY\_INVARIANTS**

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.

**CAST\_VOTE\_TIME\_PROVENANCE**

The fact that a vote has been cast within the prescribed time limits shall be ascertainable.

**CONTROLLED\_SYSTEMS\_AND\_VOTE\_INTEGRITY**

Election equipment under the control of the electoral authority shall be protected against influence that could modify the vote.

**UNCONTROLLED\_SYSTEMS\_AND\_VOTE\_INTEGRITY**

The integrity of the vote must not depend on the security of election equipment not under the control of the electoral authority.

**NO\_BREADCRUMBS**

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.

**ELIGIBILITY\_IMPLIES\_VOTE\_VOTER\_INVARIANTS**

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.

**VOTE\_CHOICE\_INVARIANTS**

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.

**END\_OF\_VOTE\_PERIOD\_INVARIANTS**

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.

**DATA\_COMMUNICATION\_INTEGRITY\_INVARIANTS**

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.

**TALLY\_INVARIANTS**

The counting process shall accurately count the votes. The counting of votes shall be reproducible.

**BALLOT\_BOX\_AND\_TALLY\_INVARIANTS**

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.

**ADVERSARY\_RESOURCES**

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.

**NATIONAL\_SECURITY**

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.

**FEDERAL\_REQUIREMENTS**

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.

**LOCAL\_REQUIREMENTS**

Reduced security requirements might be appropriate for county, municipal, or other kinds of elections

**AUTOMATED\_REGISTRATION\_FRAUD**

Automated registration fraud must not be possible.

**CLIENT\_SIDE\_AUTHENTICITY**

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

**AUTHENTICATION\_INDEPENDENCE**

The security of authentication must not be affected by any potential breach of any public or commercial databases.

**ZERO\_KNOWLEDGE\_AUTHENTICATION**

It should not be possible for an attacker to impersonate voters even if the entire server database used for authentication is compromised.

**AUTHENTICATION\_CREDENTIAL\_REESTABLISHMENT**

In some cases of security breach it must be possible to require all voters in a jurisdiction to re-establish credentials.

**E2E\_VOTE\_PRIVACY**

Vote privacy must be preserved end-to-end insofar as mathematically possible.

**VOTE\_PRIVACY\_INVIOLATE**

Vote privacy cannot be waived by voters.

**MALWARE\_PRESENCE**

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.

**REMOTE\_MONITORING**

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.)

**CLIENT\_SIDE\_CHANNELS**

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.

**SOCIAL\_MEDIA\_SIDE\_CHANNELS**

The client should not provide any information to third parties, e.g., Facebook, Twitter, etc. regarding the act of voting.

**NO\_TRACKING**

There must be no tracking devices or tracking logic in the vote client.

**NO\_BREADCRUMBS\_DETAILS**

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.

**TRANSIENT\_DATA\_CLEANUP**

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.

**FORENSICALLY\_SECURE**

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.

**REMOTE\_ADMINISTRATION\_FORBIDDEN**

The voting system should not support platforms that have remote administration or remote control tools installed that cannot be turned off by the voter.

**INVULNERABLE\_TO\_ELECTION\_MALWARE**

The voting system must not be vulnerable to malware designed to modify votes before they are input to the E2EV system.

**CLIENT\_SYSTEM\_AUTHENTICATION**

The voting system server must authenticate that it is communicating with a genuine vote client during a voting session.

**PENETRATION\_ATTACKS**

Deny penetration attacks. (more detail to be added later)

**APT\_ATTACKS**

Deny advanced persistent threat attacks. (more detail to be added later)

**INSIDER\_ATTACKS**

Something about insider attacks being impossible. (more detail to be added later)

**COERCION\_PREVENTION**

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.

**SOFTWARE\_INDEPENDENCE**

The system must witness software independence: the tabulation record must not rely solely on software.

**DIGITAL\_EVIDENCE\_NOT\_A\_RECEIPT**

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

**AUTHENTICATION\_REQUIREMENTS**

**VOTER\_AUTHENTICATION**

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).

**NO\_THIRD\_PARTY\_AUTHENTICATION**

Authentication must not be done through third party intermediaries such as Facebook, iCloud, Google, Yahoo, Amazon, etc. that offer authentication services.

**SECRET\_AUTHENTICATION\_SHARED\_SECRETS**

Authentication for remote voting systems must not use personal information, government or commercial account identifiers, etc.

**AUTHENTICATION\_DATA\_UPDATES**

Authentication secrets must be changeable or revokable at any time at the behest of either the voter or election officials.

**AUTHENTICATION\_DATA\_REFRESH\_PERIODICITY**

All voter authentication secrets must be changed at least once in every election cycle.

**CLIENT\_ENVIRONMENTS**

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.

**AUTHENTICATION\_RESILIENCE**

There must be no way to automate forging or invalidation of voter authentications without compromising the cryptographic protocols or secrets used in the system.

**OPEN\_DOCUMENTATION**

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.

**DOCUMENTATION\_CONSISTENCY**

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.

**OPEN\_SOURCE**

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.

**SOURCE\_LICENSE**

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.

**ELECTORAL\_AUTHORITY\_UPDATE**

The electoral authority has the right and ability to update election systems to conform to changes in applicable law, available technology, or the system threat model.

**CERTIFICATION\_FUNCTIONAL\_REQUIREMENTS**

**AUTOMATED\_TESTING**

Each functional requirement must have an associated set of automated tests that provide evidence that the requirement is fulfilled.

**ELECTION\_PROTOCOL\_PROOFS**

The election protocol shall have associated formal proofs of correctness and security.

**CERTIFICATION\_PROCESSES**

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.

**CERTIFICATION\_PARTIES\_COMPETENCE**

Any E2EV Internet voting system should be certified by competent professionals.

**CERTIFICATION\_REPORT\_TRANSPARENCY**

Any and all certification reports issued by certification professionals must be public, whether they recommend certification or not.

**RECERTIFICATION\_CONDITIONS**

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.

**RECERTIFICATION\_PERIODICITY**

The requirements must be re-established and recertified every election cycle even if there are no changes.

**VALIDATION\_PLATFORM\_COVERAGE**

The system must be extensively tested on a wide range of platform and software combinations.

**PUBLIC\_VALIDATION\_PLATFORM\_COVERAGE\_RESULTS**

All test procedures and results for platform coverage must be public.

**ELECTION\_TIMETABLES**

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.

**ELECTION\_PERIOD**

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.

**EVOTING\_OUTREACH**

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.

**VOTER\_VERIFIABLE\_VOTER\_REGISTER**

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.

**ONLINE\_VOTER\_REGISTER**

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.

**VOTER\_REGISTRATION\_ELECTION\_OVERLAP**

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.

**ONLINE\_CANDIDATE\_NOMINATION**

The possibility of introducing online candidate nomination may be considered.

**PUBLIC\_CANDIDATE\_LIST**

A list of candidates that is generated and made available electronically shall also be publicly available by other means.

**MULTIPLE\_CHANNELS\_ONE\_VOTE**

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.

**VOTING\_PERIOD\_INVARIANT**

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.

**UNIVERSAL\_VOTER\_HELP**

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.

**FAIR\_VOTING\_OPTIONS**

There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.

**VOTING\_OPTIONS\_ONLY**

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.

**FAIR\_VOTING\_OPTION\_INFORMATION**

If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.

**BINDING\_ELECTION\_CLARITY**

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.

**REMOTE\_RECEIPT\_FREEDOM**

A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.

**SUPERVISED\_VOTE\_RECEIPT\_FREEDOM**

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 person, or take this proof outside of the polling station.

**SECRET\_INTERMEDIATE\_TALLY**

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.

**NO\_ITALIAN\_ATTACK**

The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.

**DECODING\_LATENCY**

Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.

**TALLY\_OBSERVATION**

When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.

**TALLY\_RECORD**

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.

**INTEGRITY\_VIOLATION\_RECORD**

In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as having their integrity violated.

**SYSTEM\_AUDITABILITY**

The e-voting system shall be auditable.

**SYSTEM\_AUDITS\_IMPACT**

The conclusions drawn from the audit process shall be applied in future elections and referenda.

**OPEN\_SYSTEM**

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.

**SUPPORTED\_CLIENTS**

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.

**CLIENT\_INTERFERENCE**

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.).

**MANDATORY\_CLIENT\_TECHNOLOGY**

Operators of voting systems must document exactly what configuration choices the voter must make to successfully vote (e.g., mandate Javascript).

**PRIVACY\_ENHANCING\_VOTER\_OPTIONS**

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.

**BREADCRUMBS\_USER\_ADVICE**

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.

**PUBLIC\_SYSTEM\_MANIFEST**

The electoral authority shall publish an official manifest of the software used in an e-election or e-referendum. It may exclude from the public manifest data protection software for security reasons. 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.

**PRIVATE\_SYSTEM\_MANIFEST**

The electoral authority shall maintain a manifest of all software, including data protection software, used in the system. This manifest shall contain at least the same information as the public manifest. A procedure shall be established for updating the manifest to reflect changes to the installed software.

**MANIFEST\_ACCURACY**

It shall be possible for the electoral authority to check the installed software against the system manifests at any time.

**SYSTEM\_FAILOVER\_INVARIANTS**

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.

**DATA\_BACKUP\_INVARIANTS**

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.

**SYSTEM\_INVARIANTS\_DURING\_ELECTION**

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.

**PRE\_ELECTION\_CERTIFICATION\_INVARIANTS**

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.

**FORMAL\_CONTROL\_PROCEDURE**

All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be performed with advance notice.

**PHYSICAL\_SECURITY\_OF\_SYSTEMS\_INVARIANTS**

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.

**INCIDENT\_RESPONSE\_INVARIANTS**

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.

**OPERATIONAL\_TRANSPARENCY**

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.

**AUDIT\_SYSTEMS**

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.

**AUDITING\_COMPLETENESS**

End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities.

**AUDIT\_SYSTEM\_BASELINE**

The audit system shall be open and comprehensive, and actively report on potential issues and threats.

**AUDIT\_SYSTEM\_DATA**

The audit system shall record times, events and actions, including:

* + 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.
  + any attacks on the operation of the e-voting system and its communications infrastructure
  + system failures, malfunctions and other threats to the system.

**AUDIT\_SYSTEM\_EVIDENCE**

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.

**AUDIT\_DATA\_SECURITY**

Disclosure of the audit information to unauthorized persons shall be prevented.

**AUDIT\_DATA\_SECRECY**

The audit system shall maintain voter anonymity at all times.

**VOTER\_LIST**

The list of voters who voted online should be published.

**AUDIT\_SYSTEM\_CAPABILITY**

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.

**AUDIT\_SYSTEM\_FOR\_LEGAL\_COMPLIANCE**

The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions.

**AUDIT\_DATA\_VALIDITY**

The audit system shall be protected against attacks that may corrupt, alter or lose records in the audit system.

**AUDIT\_DATA\_CONFIDENTIALITY**

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.

**LOG\_BASICS**

The Internet voting system should keep detailed logs of all relevant activity.

**LOG\_IMMUTABILITY**

Log entries must be unmodifiable once written.

**LOG\_COMMITMENT**

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).

**LOG\_DATA\_COMPLETENESS**

The log data should be as complete as possible, consistent with maximum possible vote privacy.

**PRIVACY\_VS\_FRAUD\_TRADEOFF**

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.

**VERIFICATION\_PARTIAL\_FAILURE**

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.

**VERIFICATION\_SOURCE**

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.

**VOTER\_COMPREHENSION\_AND\_CONFIDENCE**

The electoral authority shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

**PUBLIC\_SYSTEM\_FUNCTION**

Information on the functioning of an e-voting system shall be made publicly available.

**VOTER\_PRACTICE**

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.

**OBSERVER\_INVARIANTS**

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.

**DISCLOSURE\_OBLIGATIONS**

The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.

**CERTIFICATION\_OBLIGATIONS**

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.

**RECOUNT\_SUPPORTED**

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.

**RERUN\_SUPPORTED**

The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

**RELIABILITY\_AND\_SECURITY**

The electoral authority shall ensure the reliability and security of the e-voting system.

**NO\_FRAUD\_OR\_INTERVENTION**

All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.

**SYSTEM\_AVAILABILITY**

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.

**SYSTEM\_GENUINE\_AND\_CORRECT**

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.

**SYSTEM\_AND\_DATA\_ACCESS\_CONTROL**

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.

**OPEN\_BALLOT\_BOX\_INVARIANTS**

While an electronic ballot box is open, any authorized 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.

**VOTES\_INVARIANTS**

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.

**SEALED\_VOTES\_VOTER\_RELATION**

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.

**VERIFICATION\_FAILURE\_PROCEDURES**

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.

**USABILITY\_REQUIREMENTS**

**MANDATORY\_USABILITY\_TESTING**

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.

**VOTE\_CONFIRMATION**

If a voter receives the final Thank you for voting confirmation, then she/he can be certain the ballot was recorded.

**UNCERTAIN\_VOTER\_REVOTE**

If the voter is uncertain about the state of their ballot, he/she is free to attempt to vote again.