Chapter 3

Remote Voting

3.1 Rationale

Remote voting is becoming ever more common, necessitated by a growing and diverse needs of voters. In the 1980's less than 5% of ballots were cast before election day. In the 2012 general election, 31% of all ballots were cast early and 17% were cast by mail. Remote voting is used to enable overseas citizens and military personnel to participate in elections, reduce access related discrimination domestically, and decrease expensive administrative overhead of polling locations. Some states have entirely switched over to all-mail voting, like Washington, Oregon, and most recently Colorado.

3.1.1 Accessibility

Studies issued by the International Center for Disability Information and the National Institute on Disability and Rehabilitation Research indicate that 20% of Americans live with disabilities. With this in mind, the Voting Accessibility for the Elderly and Handycapped Act of 1984 designates that any person with a disability may apply for absentee ballot without need of medical certificate.

3.1.2 UOCAVA

In 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act, stating citizens that are part of the uniformed services, merchant marines, and their families or citizens residing overseas are allowed to register and vote absentee for federal office. It is very difficult to calculate the exact number of UOCAVA eligible voters. Even so, several studies have been provided reasonable estimates. According to the two studies referenced, the states most impacted by UOCAVA are listed in **??**; which provides an estimate of the percentage of cumulative UOCAVA voters per state.

3.1.3 Domestic Absentee

Domestic absentee votes are early and mail cast by those often unable to be present at polling locations on election day. The domestic absentee vote does not include states who are completely vote by mail nor UOCAVA voters. The number of states that allow applications for absentee ballots without justification have grown to 27 as of 2015, referred to as no-excuse-absentee-voting.

Gathered from the Election Assistance Commission's 2012 General Election Administration and Voting Survey, Figure 3.2 lists the states most impacted by domestic absentee votes. These states are frequently using domestic absentee to address concerns and costs associated with administering polling locations in low population density areas.

State	**Overseas Voting Eligible Population** (McDonald 2009)	**Overseas military and federal civilian employees** (US Census Bureau 2010)
Texas	11.05%	11.78%
California	9.78%	8.44%
Florida	9.09%	9.54%
New York	5.31%	4.12%
Pennsylvania	4.10%	3.12%
Illinois	4.03%	3.24%
Ohio	3.51%	3.07%
Michigan	3.29%	2.68%
Georgia	2.84%	3.83%
Washington	2.78%	2.77%
North Carolina	2.78%	2.91%
Tennessee	2.57%	2.81%
Virginia	2.51%	3.52%
Estimated Total	4,972,217	1,042,523

Figure 3.1: Comparisons of American Overseas Population by State

State	**Percent of Population**
Colorado	71.4%
Arizona	65.9%
Montana	57.5%
Georgia	48.8%
Iowa	43.1%
California	39.8%
Hawaii	36%
North Dakota	28.8%
Florida	26.8%
Michigan	26.4%
Wyoming	26.2%
Maine	25.5%
Nebraska	25.4%
Idaho	24.3%
Ohio	22.4%
Wisconsin	21.4%
Vermont	20.4%

Figure 3.2: Votes Cast as Domestic Absentee 2012 General Election

3.1.4 Expectations

In 1952 there was an American Political Science Association special study of voting in the armed forces intended "to be sure that we have a completely effective program for voting in the armed services." From this activity ten voting rights were clearly defined. These rights are:

1. To vote without registering in person.
2. To vote without paying a poll tax.
3. To vote without meeting unreasonable residence requirements.
4. To vote without meeting unreasonable literacy and educational requirements.
5. To use the Federal postcard application for a ballot.
6. To receive ballots for primary and general elections in time to vote.
7. To be protected in the free exercise of their voting rights.
8. To receive essential information concerning candidates and issues.
9. To receive essential information concerning the methods by which the right to vote may be exercised.
10. To receive essential information on the duty of 'citizens in uniform' to defend our democratic institutions by using, rather than ignoring, their voting rights.

The Help America Vote Act (2002), defines new mandatory minimum standards for states to follow, to specifically address access related concerns raised in the 2000 presidential election. This act defines the need to support multilingual and disabled persons for elections by providing the same opportunity for access and participation (including privacy and independence). Additionally, persons who have questionable voting eligibility must be permitted a 'provisional ballot.'

Finally it is most important to include the expectation that votes cast by registered voters are counted correctly while preserving privacy. As will be mentioned later in this chapter, there are many examples where this isn't the case.

3.2 History

3.2.1 Armed Forces Voting

Before the civil, war US citizens primarily voted in their places of residence, and many states legally barred the casting of votes from outside state borders. There was little effort from any state to accommodate absentee voting. However, in 1864, with the American Civil War displacing soldiers from their residences, Lincoln's re-election was at risk. With much lobbying on behalf of the republican party (and opposition from the democratic party), nineteen of the union's states adopted absentee voting procedures for military voters on federal elections in time for the election. Unfortunately since the motivation to passing these laws was securing Lincoln's re-election, rather than persistent enfranchisement, many absentee military voter laws were treated as temporary and repealed after the war.

In 1918 America's War Department decided that it was not ready to support the military vote. World War I had displaced such a large number of voting eligible persons and military units were rarely composed of same state citizens. Not even states in support of military vote were allowed the soldier vote, even on matters at the state level.

As in the Civil War, World War II inspired another push for the military vote in hopes of supporting the re-election of the presidential incumbent. This introduced the Soldier Voting Act (1942) which, although passed too late for the presidential election, mandated military personnel rights to absentee vote on federal elections during times of war without subjugation to voting tax or postage costs. From this point forth all overseas voting would be regulated at the federal level and implemented at the state level. However, by 1944, the state mandate to support military absentee voting was amended to a recommendation.

3.2.2 Remote Civilian Voting

Progress for civilian absentee voting lagged the armed forces. In 1896, states began introducing civilian absentee voting legislation. By 1924 only three states in the union had no absentee voting legislation, but all states had different laws and restrictions. Major progress on this front wasn't made until federal voting laws were passed that enabled both civilian military votes. The Voting Assistance Act of 1955 was the first to federally combine voting policy recommendations for overseas civilian government employees with military.

With lobbying from sympathetic groups and a growing population of overseas civilians, Overseas Citizens Voting Rights Act passed in 1974 to extent the vote to citizens regardless of their intentions to return to the United States.

In 1986, the Voting Assistance Act was amended to include individuals temporarily living outside the United States. By this time, combatant attitudes towards overseas votes had finally settled, and the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) was passed. This act combined and replaced the Federal Voting Assistance Act, and finally made supporting the overseas absentee ballot a requirement.

3.2.3 Disabled Civilian Voting

The Voting Rights Act (VRA) of 1965 was the first legislation to enfranchise voters with disabilities. The VRA granted voters who require assistance to vote by reason of blindness disability or inability to read or write assistance by a person of the voters choice. This also introduced some of the earlier legislation defining a disabled citizen.

The Voting Accessibility for the Elderly and Handicapped Act of 1984 (VAEHA) was passed to improve access for handicapped and elderly individuals. However, states were left to set their own standards of access, and limited the disabled voters group to those with *physical disabilities*. The VAEHA did, however, mandate 'no notarization of medical certification shall be required of a voter with a disability with respect to an absentee ballot or application for such ballot.'

The 1990 American Disabilities Act (ADA), required that people with disabilities have access to basic public services, including the right to vote. However, this law does not strictly require that polling locations are accessible. ADA did however extend the definition of disability to:

> "a person who has a physical or mental impairment that substantially limits one or more major life activities, a person who has a history or record of such an impairment, or a person who is perceived by others as having such an impairment."

The majority of federal laws passed to protect voting rights of disabled citizens have struggled to clearly define an representative range of disabilities, and are often focused on access at physical polling locations; which is expensive for states to implement. Additionally, state defined policies often ignore rights to voting privacy, and exclude persons with multiple disabilities sighting that aiding technologies are not yet available.

3.2.4 Modern Remote Voting

In 2002 Congress passed the Help America Vote Act (HAVA) partially as response to problems found in gathering, counting, and auditing votes in the 2000 presidential election. HAVA required that all polling places in elections for federal office, anywhere in the United States have at least one voting system enabling disabled voters, addressing some accessibility concerns.

HAVA also attempted to address concerns raised by the large number of rejected critical ballots in 2000, due to an inability to sufficiently audit ballots. This act advises voting technologies to produce a Verifiable Voter Paper Audit Trail (VVPAT); while preserving the privacy of the voter and the secrecy of the cast ballot. The Federal Election Assistance Commission (EAC) was created to oversee the development of new voting machine standards, and released the Voluntary Voting System Guidelines to aid in this transition.

Today legislation on absentee voting has been a slow moving event. Existing voter rights regulations are enforced at a state level and are hampered by local political attitudes.

3.3 Shortcomings of Current Practice

There are many concerns with current election practices that an E2EIV system could help to mitigate. The topics listed below draw from specific concerns that have a large impact on remote voting participants.

3.3.1 Use of Communication Technologies

The majority of remote voting is performed by 'vote-by-mail' which is subject to many inherent faults that only become more problematic for UOCAVA's overseas voters. The 2008 Post-Election UOCAVA Survey Report and Analysis found that 52% of attempted UOCAVA votes were not counted, due to problems in the mail delivery process.

Due to the many states' diverse registration practices, the Federal Voting Assistance Program provides an accompanying Voting Assistance Guide to registration forms. Unfortunately, this is very large and difficult to follow. For states without a streamlined online registration (hosted by OVF), this has resulted in many failed voter registration attempts.

3.3.2 Accessibility and Usability

In 2007, 20% of Americans with disabilities said they were unable to vote in presidential or congressional election due to barriers at or getting to the polls. This is frequently a consequence of the voting technologies used and the physical location of polling places. In the 2000 presidential election, 56% of randomly sampled polling places in the United States had at least one identified impediments for disabled voters.

Disabled persons often forfeit privacy to appointed aids,often as result of insufficient technology support at polling locations. Those with dexterity impairments often have problems with handling and marking paper ballots (at polling places and at home).

3.3.3 Auditing

Although it is believed that voter fraud is fairly uncommon, it is a major concern in a bipartisan system. Unfortunately, it is very difficult to detect without verification technologies. Often, policies intended to reduce fraud or protect identities result in a higher rate of rejected ballots. According to the 2012 Election Administration and Voting Survey, 17.6% of absentee ballots were rejected due to non-matching signatures.

Privacy of vote is a strong expectation of a fair voting system, that is often left unaddressed. Most practices for UOCAVA voters forfeit independent or private voting, with several states even requiring a voter privacy waver to be signed for remote ballots. In several jurisdictions, UOCAVA votes are not counted until it is determined that they may sway the election. [1]

[1] citation needed

Chapter 4

E2E VIV Explained

4.1 Goals

Typical Internet voting election processes have six phases:

Setup During the setup phase, the election officials gather the information needed to run an election. This includes gathering registration information for all voters, identifying the issues and races that will be voted on, designing and specializing ballots, sending instructions and other information about the election to voters, and so on.

Distribution Once the election has been set up, election officials must distribute ballots to the voters. Different voting system architectures use different mechanisms, including postal mail, email, or by having voters interact with a website.[1]

Voting Voters then fill out their ballots, often with the help of software installed on their own computers.

Casting Filled out ballots are then returned to the election officials; as with distribution, different architectures use different mechanisms.

Tallying The tallying phase includes the remainder of the election finalization tasks: counting votes and announcing the election outcome are common to almost every process, though some include other miscellaneous tasks like publishing certain information needed for audits.

Auditing Some elections will inevitably be disputed; in such cases, there is a final phase in which interested parties look for evidence that the election outcome is correct (or not!).

One major concern for Internet voting involves ballot integrity during the distribution, voting, and casting phases. For the election outcome to be correct, it is important that the ballot that is received by and displayed to the voter match the ballot that was created and sent by the election officials; that the computer used to fill out the ballot faithfully reports the intention of the voter; and that the filled out ballot be received by the election officials exactly as it was when it was sent by the voter. Typical Internet communications involve not just the computers owned by the two parties communicating, but also many intermediary computers controlled by neither party. A good election system needs to account for this, making it impossible for these intermediates to intercept ballots for viewing or modification during transit. Another concern is that voters computers are rarely administered by experts, and as a result many of them are compromised by outside forces. One consequence of this is that the voting phase itself may become corrupted: even if the ballot arrives unchanged at the voter, malware on the voter's computer may change the way the ballot is

[1] We distinguish between sending instructions to voters and distributing ballots; there is no hard and fast rule for the distinction, but a rule of thumb is that instructions are applicable to many voters, whereas anything that has been specialized for a single voter is part of the ballot and falls under the distribution phase.

displayed or the way the vote is recorded before casting the vote. It can be difficult to design a system that is resistant to this kind of attack without seriously sacrificing the usability of the system. Some systems use alternative distribution mechanisms as cross-checks; for example, sending something to the voter by postal mail which can be used to check that the ballot displayed by their computer is correct.

To the extent that it is possible, it is desirable for Internet voting to be private and anonymous. Voters should feel comfortable voting the way they like (and not feeling pressured to vote for a particular candidate or to vote a particular way on some issue); the fewer people who know or can find out the way a given voter voted, the more comfortable they can feel. On the other hand, election officials only want to record votes from people who are registered to vote, and even then want to record only one vote from each voter. Thus there is a tension during the vote casting phase between retaining the anonymity of votes and ensuring that a vote is coming from somebody who ought to be able to vote.

One popular approach to this problem in existing systems is to initially require each vote to be tied to the voter who cast it long enough to decide whether to include the vote in the later tally or not; then to keep the vote but delete the information about who cast the vote. This approach can work; however, audits of systems that take this approach shows that it is all too easy to accidentally retain the connection between votes and voters longer than intended, and make this information much more widely visible than intended. From the privacy side of the tradeoff, it would be better if the voter could be confident that there was no connection stored because the information they send to the election officials during the casting phase does not include any personally identifying material.

There is a subtle distinction being made here. We certainly want our Internet voting systems to be correct, private, secure, and so forth. It is important for the people developing these systems to verify that they are correct and take an active role in seeking out and eliminating defects in the system. But the goal of verifiable Internet voting is to go even farther: not just correct, but *visibly* correct. That is, it must be possible for the parties using the system to be able to *check* that the system is behaving correctly, without trusting in the abilities of the people who created the system to avoid bugs or trusting in the inability of third parties to influence the behavior of the system. As applied to anonymity: since it is not easy to prove to somebody else that you have deleted some information, one must simply avoid giving them that information in the first place. This theme—of being not just correct, but verifiable—is one of the central ones of verifiable Internet voting, and is a critical part of the defense against the software bugs, security vulnerabilities, and sophisticated cybercrimes that history tells us are sure to crop up.

The tallying process provides a particularly good example of the difference between correctness and verifiability. We certainly want the election system to count the votes correctly; but the goal of verifiability is to provide some evidence to voters that the election outcome is correct. For example, some systems allow voters to check that their vote was included in the election outcome; some allow voters to check that the system is recording the content of their votes correctly; some even allow voters to check that the number of people that voted for a given candidate is accurately calculated without revealing any of the individual votes. Meeting these verification goals without violating the anonymity and privacy goals can be a balancing act.

Each of these individual goals contribute to a single top-level goal: end-to-end verifiability. The "end-to-end" property is that the whole election process produces a result that matches the intentions of the voters. The subgoals of this are summarized with the catchphrase, "Cast as intended; recorded as cast; and counted as recorded." This recapitulates the concerns discussed above; "cast as intended" is the demand that casting use secure communications and other mechanisms to ensure that malware and outsiders cannot change the vote, "recorded as cast" is the demand that the election system itself correctly interprets a vote, and "counted as recorded" is the demand that the tallying process be faithful; and all of these demands are subject to not just correctness but verifiability, so that a voter can convince themselves that these properties hold even if they suspect that the system or election officials have been corrupted.

4.2 Shortcomings and Expectations of E2EVIV

As discussed in Chapter 3, there are several difficulties with current voting processes: voters with disabilities cannot vote unassisted, communication channels with remote voters are slow and unreliable, vote tallying is labor-intensive and error-prone, and election audits are costly. Additionally, there is little visibility into the election process, meaning that individual voters and, in some cases, even auditors, must trust the reports of election officials and voting hardware

vendors on election outcomes and processes. Internet voting may be able to alleviate some of these concerns. Voters with disabilities could potentially use their own familiar hardware, such as Braille displays, screen readers, sip-and-puff input devices, and so on, to participate in the election. Internet communications are traditionally speedy (seconds per message rather than weeks) and relatively robust compared to overseas postal mail. In most systems, tallying is automated and fast. Auditing can still be a challenge, though there is some hope that verifiable systems can make elections more transparent for this purpose, too.

There are also some serious challenges in rolling out an Internet voting system. Chapter 7 discusses the feasibility of producing a system that meets the security and verifiability goals we have touched on above. In addition to those concerns, the ability of normal voters to use the system to cast their vote in the way they intend to vote is a major goal; as we discuss below, current systems do not meet this goal very well. One component of this is the system itself; though another that is common to all Internet voting systems is the need for voters to have Internet access. This is not necessarily possible for all overseas and military voters.

4.3 E2E VIV in Practice

A number of practical voting systems have been developed based on the principles of E2E VIV. This section describes several systems that have been used in a real election or in a pilot.

4.3.1 RIES [22]

RIES, the Rijnland Internet Election System, was first used in 2004 to support elections to the Rijnland water management board, supplementing the system of postal voting used by the water board. A subsequent version was used to allow expatriate voters to participate in the Dutch parliamentary elections [20].

Before a RIES election, credentials are mailed to every voter in the form of a very long number. The same mailing also includes instructions for the voter.

During the election, voters log into an election web site that includes a client-side voting application written in JavaScript. The client-side application encrypts the vote by passing the voter authorization code and the public ID of the candidate through a one-way function to create the encrypted vote. The encrypted vote is then placed on a public bulletin board that serves as a ballot box.

At the close of the polls, the election authority releases the final vote tallies along with a codebook containing the encryptions of all valid credentials with all candidate IDs.

The algorithms and protocols used RIES are public, and each voter, having access to all of the inputs and outputs, may (in principle) check the computations. This is weaker than the desired individual verifiability, but nonetheless, far stronger than conventional voting systems.

The Organization for Security and Co-operation in Europe (OSCE) sent an election assessment team to observe the use of RIES in 2006. Their report contains observations of critical security features of the system that could not be observed [24]. Further weaknesses were revealed by the Eindhoven Institute for the Protection of Systems and Information (EiPSI) in 2008 [23], notably that:

- the procedure of voter self-check is quite complicated,
- the two-channel (mail and Internet) voting makes system less transparent,
- too much power is given to the election administrator and the system's Internet host,
- issues arise when modifying the codebook due to a revoked ballot, and
- there are realistic ways to forge votes via cryptographic hash collisions.

One of the more important lessons learned through RIES is that when voter authorizations are distributed long in advance of the election, a mechanism must be provided allowing voters to obtain replacement credentials and invalidate lost credentials. These mechanisms add significant complexity to system, and is a source of some of the problems reported in the OSCE and EiPSI reports.

Another feature of RIES rife with tradeoffs is the ability to perform testing during the election: pre-invalidated test ballots are deliberately added to the bulletin board in order to test the network path from selected Internet clients to the server. While such testing in principle can increase confidence in the election integrity, in practice it opens the system to spoofing and denial of service attacks. Furthermore in the RIES implementation the system is aware of the fact that it is processing a testing ballot, and all of the test ballots were voted identically from the same computer, limiting the confidence added at the expense of these vulnerabilities.

In the wake of these critical reports, plans to use RIES in the 2008 Dutch parliamentary elections were scrapped, and Internet voting as a whole was banned in the Netherlands.

4.3.2 Prêt à Voter [12]

The state of Victoria in Australia held a governmental election in November 2014, using a version of the Prêt à Voter system [7]. An attempt was also made to use Prêt à Voter in a student election at the University of Surrey in February 2007 [5]. The failure of this attempt illustrates many of the pitfalls of adapting a research system to an actual election, such as a short timetable, a lack of clear requirements, and the need for rigorous implementation practices.

Prêt à Voter uses two-part paper ballots with the candidate names on one part and the voting targets plus a ballot ID number or barcode on the other part. Typically, the two parts are printed as a single sheet with a perforation to divide the sheet after voting.

From the voter's perspective, the order of the candidate names on the ballot appears to be random. The voter marks her choice next to the candidate name of her choice, separates the two parts of the ballot, and destroys the candidate names. She may take a copy of the voted part home for later verification.

For tabulation, there is a cryptographically secure mapping from the ballot ID numbers to the apparent random order of the candidate voting positions. Multiple custodians using a mixnet or similar technique use this mapping to decode cast ballots into anonymized plain-text ballots which are then posted to a bulletin board.

Unvoted ballots may be audited before, during and after the election to ensure that the decoding of cast ballots is being correctly performed. Randomly selected stages in the decoding can be challenged to prove the integrity of the count, and the plain-text decoded ballots are easily counted for verification by any interested party.

An individual voter may also search for their voted ballot ID on the bulletin board. This reveals the positions that were marked on that ballot, but crucially, it does not show the corresponding candidate names. The voter may therefore verify that the positions marked at the polling place were correctly recorded by the election officials, but because the voter no longer has the part of the ballot linking candidate names to ballot positions, the voter cannot prove to anyone else how the ballot was voted.

4.3.3 Punchscan [26, 27]

Punchscan was used for the graduate student association elections of the University of Ottawa in 2007 [17]. It is likely the first E2E voting system with ballot privacy used in a binding election.

The election experience for a Punchscan voter is very similar to that of Prêt à Voter. The system uses a two-part paper ballot where the top part has candidate names and candidate numbers (or letters) and the bottom part has numbered (or lettered) voting targets. Holes punched in the top part expose the voting targets below. The order of the voting targets for each race appears random to the voter. Both halves of the ballot bear an identical serial number.

The voter casts their vote by marking her choice with a bingo dauber, and the two halves are separated. Either side can be scanned (since the bingo dauber marked both through the hole and around it) as the cast ballot. The other side is destroyed, and a copy of the cast side may be retained by the voter.

A curious voter may inspect the public record of any cast ballot exactly as with Prêt à Voter. It does not matter which half of the ballot the voter retained, because there is no public display of the numbers that link candidate names to voting positions; only the position that was marked is displayed. Again, individual ballots may be audited, and the key to tabulating the votes is that there is a cryptographically secure mapping from the ballot serial numbers to the apparent random order of the candidate voting positions.

4.3.4 Scantegrity II [14, 15]

Scantegrity II (Invisible Ink) was used in the Takoma Park, Maryland municipal elections in 2009 [9]. In 2011, it was used for in-person voting with Remotegrity (4.3.5) used for absentee voting. The 2009 Takoma Park election was the first use of an E2E system with ballot privacy in binding governmental elections.

Before the election, officials generate the seed to a pseudorandom number generator using a secret sharing scheme. Three-letter alphanumeric codes are created for each choice on each printed ballot using this seed, and additional tables are created so that interested parties can later confirm that the tally was computed correctly.

During the election, the voter experience is nearly identical to that of conventional optical-scan paper ballots. When the voter marks their choice, the ink in the pen reacts with invisible ink on the paper to disclose the three-letter code in the marked voting target. The ballot ID number and the displayed code are posted to a public bulletin board.

After the election, public verification of the final tally proceeds with the public bulletin board in a manner similar to that of Punchscan and Prêt à Voter.

In addition to the public verification, an individual voter who takes note of their ballot ID number and the code revealed from invisible ink may use the public bulletin board to check that their ballot was indeed tabulated, though this information is not sufficient to prove that they voted a particular way.

4.3.5 Remotegrity [32]

Remotegrity is a remote coded voting system that was used for absentee voting alongside Scantegrity (4.3.4) for in-person voting for the 2011 Takoma Park, Maryland municipal elections.

Remotegrity voters receive a coded voting ballot and an authentication card in the mail. The codes on the ballot can be covered by a lottery-style scratch-off field. The authentication card contains several authentication codes under scratch-off, a lock-in code under scratch-off, and an acknowledgment code. Both cards have serial numbers. The voter can be sent two ballots so that she can use one for auditing purposes.

To vote, the voter enters both serial numbers, the codes corresponding to her choices, and an authentication code obtained after scratching-off a surface chosen at random.

She returns to the election website a few hours later to check if her codes are correctly represented, and to see if the election authority has posted her acknowledgment code next to the codes. This indicates to her that the election officials received valid codes for her ballot.

She scratches off the lock-in code and posts it on the website. This affirms to the election officials, observers and other voters that her vote is correctly represented on the website.

Among all of the systems discussed here, this is the first one that asks the voter to take positive action to confirm that the vote was correctly posted.

As with RIES, if we assume that there is no communication between the computer used to print the credentials and the computer used to collect the votes, the latter computer does not know the mapping from codes to candidates, so the vote is not revealed to the computer. Further, because the computer does not know a valid code corresponding to another candidate on the ballot, it cannot change the vote. Finally, and uniquely, because the computer does not know the acknowledgment code, its presence on the election website assures the voter that the election officials received a valid code for her ballot.

The tally is computed from the codes in a verifiable manner that corresponds to the coded voting system used.

If a jurisdiction is nervous about using the Internet for remote voting, Remotegrity ballots can be mailed in, and voters can check for their codes on the election website to be assured that their vote correctly reached election officials.

4.3.6 Helios [2, 3]

Helios is a system developed for web-based Internet voting. It was used for the election of a Belgian university president in March 2009 and by numerous universities and associations since then, including the Association for Computing Machinery and the International Association for Cryptologic Research.

Before a Helios election, officials input the email addresses of the voters who will be participating. The system emails the voters their randomly-generated login information and the link to the election website.

During the election, the voter enters their choices on the website. After entering her choices, the voter has an option to spoil their ballot in order to verify that it was recorded correctly. Upon completing a non-spoiled ballot, the system sends an email confirming the receipt of their vote, though not their choices. At any time before the close of the election, the voter can repeat these steps and the new vote will replace the old vote.

After the election, Helios uses homomorphic vote tallying with the optional addition of mixers and mixnets in some derivatives [6, 31].

Voter authentication is not required until after the voter decides to cast the ballot, so any interested party may prepare and audit ballots. All cast ballots are posted in encrypted form on a public bulletin board so that voters may check that their ballots have been correctly recorded. Similarly, after the polls close, the decryption and vote tally may be checked.

4.3.7 Norwegian System [19]

Between 2011 and 2014, the Norwegian government ran an Internet remote voting trial using a cryptographic protocol designed by Scytl, a commercial voting system vendor. Scytl and the Norwegian government assert that this is an E2E system, which if accurate is the first effort by commercial voting system vendors to enable E2E elections.

The Norwegian system uses a three-channel model involving postal mail, the Internet, and SMS text messaging. Before the election, the voter receives authorization codes to cast a ballot via postal mail.

During the election, the voter uses a computer to cast an encrypted ballot. The voter can cast multiple ballots; only the last ballot cast is counted, and if a voter votes both on paper at a polling place and by Internet, the paper ballot overrides the Internet ballot. After casting a ballot, the voter receives a confirmation code offering a partial end-to-end proof via an SMS message.

Available descriptions of the Norwegian system are incomplete, so it is not possible to analyze the system in depth. However the system's claims to protect voter privacy are weak: "If the voter's computer and the return code generator are both honest, the content of the voter's ballot remains private." In addition, the receipt delivered to the voter proves only that the encrypted ballot was received as cast, not that it was counted as cast or that the encrypted vote matches the voter's intent.

The system evolved significantly between its first use in 2011 and 2013, with added complexity to attempt to assure voters that their ballots were stored as cast. In 2013, the Carter Center mounted a serious effort to observe the Norwegian system in action. Their report on the operation of the system and the problems they had observing it offers useful insight into the administration of E2E systems in general as well as the particulars of the Norwegian system [10].

4.3.8 Wombat [21]

The Wombat voting system has been used for multiple pilot elections in Israel. It is an in-person voting system where the voter votes on a touch-screen and obtains a printout of her vote with an encryption of it. The voter can choose to cast or audit the encrypted vote. If she chooses to audit the vote, she may check if the vote was correctly encrypted. If she chooses to cast it, the ciphertext is posted online, and she casts the unencrypted vote in the ballot box (this may be manually counted) and takes the ciphertext home. The votes are tallied using a verifiable mixnet.

4.3.9 DEMOS [16]

DEMOS is a coded vote system where the voter is given a two-part coded ballot; she audits one part and uses the other to vote. Associated with each choice on the ballot is a vote code—the encryption of the vote, which is entered in the voting machine by the voter, and a receipt code which the voter does not enter, but which is posted online next to the vote code.

The voter can check the receipt to ensure her vote reached the election authorities. The ballot also has a QR code containing all the information on the ballot which can be scanned by the voter if she prefers not to manually enter the vote code. Once the ballot is entirely represented on the computer, the voter can then make her choices. Note that if the voter scans the QR code, the scanning computer knows how she voted. The vote codes represent homomorphic encryptions of the votes and the verifiable tally is obtained in a standard manner.

A pilot study of DEMOS was carried out during the 2014 European Elections in Greece.

4.4 Limitations of Existing Systems

E2E systems inherit many of the limitations of traditional voting systems. Reliability of equipment, reliance on procedure, trust in insiders, and accessibility are all problems with traditional in-person voting systems. For remote systems, the integrity of postal systems, turnaround time for mailed materials, access to Internet or fax technology, and reliability of Internet servers are all well-documented obstacles to voting.

Existing E2E systems mitigate some of these limitations. For example, code voting limits the ability for attacks against postal mail systems to change the candidates marked on voted ballots. However if an attacker simply intercepts and destroys the voted ballot, a replacement might not arrive in time for that voter to participate in the election. To mitigate this, election officials might choose to instead accept voted ballots via fax, email, or website, but such expedient measures often trade off the verifiability that makes an E2E system desirable in the first place.

In this section, we examine the limitations of E2E systems with a particular focus on the limitations that are unique to or exacerbated by E2E characteristics.

4.4.1 Voter Secrecy

Systems like Prêt à Voter (4.3.2) and Punchscan (4.3.3) rely on a randomized candidate order or a code on printed ballots to ensure voter secrecy. Voted ballots must appear on a public bulletin board in order to verify the election results, and so to protect secrecy only the selected position or code is visible on the final ballot along with a ballot ID.

If an insider is able to review the printed ballots before the election, they can record how the candidate positions are arranged for each ballot ID and therefore identify which candidate is marked on the voted ballots, thus violating secrecy [7].

Recent writing on Prêt à Voter recommends printing ballots on demand at polling places in order to limit this possibility [29]. Printing on demand introduces additional problems and expense compared to centralized printing. More printing equipment is required at each polling place, that equipment can break or be difficult to operate, and the printing equipment must have some way of communicating with the rest of the election infrastructure to ensure it has, for example, the correct cryptographic seeds for generating new ballots.

Scantegrity II (4.3.4) uses invisible ink to hide the vote codes on unvoted ballots, and Remotegrity (4.3.5) can use scratch-off fields to hide vote codes and other information required to cast a ballot. These techniques limit the opportunity for insiders to learn secrecy-compromising information without being detected through the presence of a marked or damaged ballot.

Even with techniques to mitigate insider foreknowledge of the ballots, secrecy still can depend on voters and poll workers correctly following procedures. A voter can leave the polling place with a complete Prêt à Voter ballot, for example, failing to shred the half with the candidate order. With both halves of their ballot, they can prove how they voted, losing receipt-freedom.

RIES makes a deliberate secrecy tradeoff by weakening the receipt-freeness requirement in exchange for providing universal verifiability and a degree of individual verifiability. The results of an entire election can be independently audited with only the information publicly available after the election. However if a voter discloses her credential or her encrypted vote, the same public information may be used to violate ballot secrecy. The developers of RIES judged this violation to be no more severe than the threats to ballot secrecy inherent in postal voting, and therefore worth accepting for the benefit to verifiability.

4.4.2 Ballot Stuffing

As when ensuring voter secrecy, many E2E systems depend on correct procedures to defend against ballot stuffing. For example, during the University of Ottawa elections using Punchscan, more ballots were cast than voters recorded in the pollbook. In this case, ballot stuffing can be caught after the fact by poll workers, but is not an inherently verifiable property of the system, and requires trust in the accuracy of the poll workers.

In the Helios system, officials can enter voters by email address, and so there is limited protection against insider ballot stuffing. Helios relies on individual voters verifying their votes, with little provision for an interested party to verify the entire election, making it difficult to detect this type of fraud [30].

A pre-election step that publicly publishes tables of valid ballot IDs can help mitigate this problem, but also creates others. All votes in the final tally have an (anonymized) provenance that can be traced back to before the election began and presumably cross-checked with voter registration rolls. However having a fixed set of ballot IDs can make it harder to replace lost, stolen, or spoiled ballots, or to providing for late or same-day voter registration.

4.4.3 Infrastructure & Equipment

Election equipment fails in practice. An E2E system must be resilient to failures while not giving up E2E properties. A system that lacks robust fallback mechanisms is not itself robust, but is only as strong as its weakest fallback. For example, if a remote voting website fails and election officials resort to accepting voted ballots by email, E2E guarantees are lost for all of the emailed ballots.

In addition to being more sensitive to failures, verifiable election systems often require more sophisticated equipment than traditional systems. For in-person voting, a verifiable system might require ballots to be printed on demand, a high-quality shredder for two-part ballots, and more sophisticated assistive devices. This complexity incurs additional cost and poll worker training requirements.

Many E2E systems post encrypted ballots during an election to a public bulletin board. In order to update the bulletin board in real time, these election systems are distributed systems, networked via traditional means or via a manual air gap. Depending on the networking scheme this can open equipment to distributed denial of service (DDoS) attacks, network partitions, inconsistency, and other problems inherent to distributed systems.

Internet systems compound the difficulties of distributed systems by requiring the systems to be accessible via the public Internet, increasing the possibilities for DDoS and other malicious attacks. Furthermore, many systems allow voters to use their own computers to vote, leading to pitfalls inherent when election officials lack control over the voting environment. Malware on the voter's computer might undermine security, incompatibilites might arise due to operating systems or web browser versions, and the network infrastructure between the voter and the central election system might be compromised with a man-in-the-middle attack.

4.4.4 Usability

Traditional election systems struggle with usability. Verifiable systems add more steps and complexity, making usability even more difficult. The mechanics of marking a ballot become more complex with code voting as in Remotegrity, and position or shape matching as in Prêt à Voter and Punchscan. Individual verification, not even possible in traditional systems, is an entirely new process that voters must master to take full advantage of E2E guarantees.

In 2014, a team of researchers from Rice University undertook a quantitative, experimental study of the usability of Helios, Prêt à Voter, and Scantegrity II [1]. They aimed to quantify usability using the ISO 9241-11 standard axes of effectiveness, efficiency, and satisfaction. Their results show that these systems broadly fail on these axes even for typical voters who are uninterested in performing additional verification steps.

The Rice study found the systems were not effective as significant number of voters failed to cast a ballot with each system. Troublingly, many of those voters thought they had in fact successfully cast a ballot; in a real election they would have left the voting process unfinished without even knowing to ask a poll worker for assistance. By contrast, traditional systems have near-100% success rates [8].

The systems also lacked efficiency, as they all required significantly more time – almost twice as long – to complete as a traditional system.

The usability of an election system is crucial for that system to not disenfranchise voters, and for voters to generally have confidence in the election results. The Rice study shows that adding E2E guarantees can be a Pyhrric victory when the resulting system is unusable for non-expert voters.

4.4.5 Accessibility

There are ability requirements for many E2E systems in various stages of the voting process. For example, a sighted voter is able to see the correspondence between candidate position and marking position on a Punchscan ballot, but a non-sighted voter cannot without assistance. In addition to obstacles to marking a ballot, some schemes with individual verification lack provisions for disabled voters to participate in individual verification without assistance. Information required for verification is frequently delivered through a paper receipt, an invisible ink code, or requires writing down receipt data.

Accessible verification protocols have been proposed that take care to protect voter secrecy and allow participation in individual verification [13]. However, these protocols require using accessibility equipment with an audio, sip-puff, or switch interface to read and mark the unencrypted ballot. The device must therefore be trusted not to record the votes, which would violate voter secrecy. The device must also represent the ballot faithfully to the voter so that votes are recorded as intended.

Requiring trust in assistive devices is not unique to E2E systems [28]. In non-E2E systems, though, trust is already widely distributed. In the context of having to trust the chain of custody of ballots, the integrity of poll workers, and the outcomes of any audits, having to trust an assistive device is a relatively small concession to make in an already-flawed system.

On the other hand, a well-designed E2E system requires a much smaller base of trust for voters to have confidence in the results of an election. By requiring an expanded base of trust in order to be accessible, the existing E2E systems undermine their E2E properties.

4.4.6 Social & Political

Novel election systems face a difficult bootstrapping problem: in order to be adopted in large-scale elections, they must have a successful track record. However in order to build up that track record, systems must be successful despite the limited resources available during small-scale pilot programs. With limited resources, corners are cut in the implementation of the election system leading to a greater chance that problems with equipment, software, and support will undermine confidence in the system.

This confidence in election systems generally, and E2E systems in particular, is fragile in the eyes of the public. When election systems fail during an election or are revealed to have substantial integrity issues, the perception of all similar systems is tainted, no matter the differences between specific systems or the reassurance of E2E guarantees. Failure of a legacy computerized system can poison the well and make the public reject a novel system by association.

For example, The Federal Constitutional Court of Germany issued a decision in 2009 in the wake of a hacking demonstration on electronic voting machines used in previous elections [18]. They decided that electronic systems may only be used in elections if "the result can be examined reliably and without any specialist knowledge of the subject", a standard which E2E systems have not been able to meet in practice [8]. Similarly after reports critical of RIES, a popular movement successfully advocated for a ban on Internet voting in the Netherlands.

Broader computer security concerns are becoming topics of household conversation with vulnerabilities like Heartbleed and droves of personal data compromises making the headlines. These concerns rightly make the public wary of any system with a computerized component, even if the Internet is not involved. The challenge for E2E systems is to overcome this broader skepticism by demonstrating integrity in a way accessible to non-experts without making it more difficult to vote.

Chapter 5

Required Properties of E2E Systems

We now describe the required properties that E2E VIV systems must have in order to be considered for use in real elections. These requirements can be broadly divided into two groups: *technical requirements* and *non-functional requirements*. Technical requirements are those that can be directly addressed by the design and implementation of the system, such as authentication requirements for voters and election officials. Non-functional requirements are those that are imposed on the system by external entities or where the system depends on external behaviors outside its control, such as specific election certification guidelines and operational procedures. Each of these groups is itself divided into several categories, and Figure 5.1 gives a high-level overview of these.

The following is a high-level description of the categories and many of the requirements within each; Appendix A contains a complete listing of all E2E VIV system requirements expressed in the Business Object Notation.

5.1 Technical Requirements

There are ten categories of technical requirements for E2E VIV systems: functional, accessibility, usability, security, authentication, auditing, system operational, reliability, interoperability, and certification.

5.1.1 Functional

The functional requirements of an E2E VIV system deal primarily with the casting and recording of ballots and associated voter records. One important requirement is that there must be a correspondence between the recorded ballots and the voters that are listed as having voted; a ballot cannot be recorded without a voter casting it, and a voter cannot be listed as having voted without casting a ballot. Similarly, if a voter is informed by the system that her ballot has been successfully cast, the system must correctly retain the record of her having voted and her cast ballot information even in the event of server failures.

Another functional requirement is the property of *receipt freedom*: it must be impossible for a voter to prove to anybody any information regarding how she voted her ballot, beyond what can be mathematically deduced from the final distribution of votes. For example, if a referendum passes with 100% of the vote, there is no way to hide the fact that every voter approved of the referendum; however, if the result is mixed, it must be impossible for any individual voter to prove how she voted. This must be the case even when the voter can create digital evidence of her actions by, for example, video recording the ballot casting process or photographing a completed ballot.

In some elections voters are allowed to cast multiple ballots with only the last cast ballot counting toward the final election tally, while in others voters are prohibited from casting multiple ballots. The system must accommodate both of these election formats, ensuring that only the last cast ballot is counted for each voter when multiple ballots are allowed and ensuring that each voter casts at most one ballot otherwise.

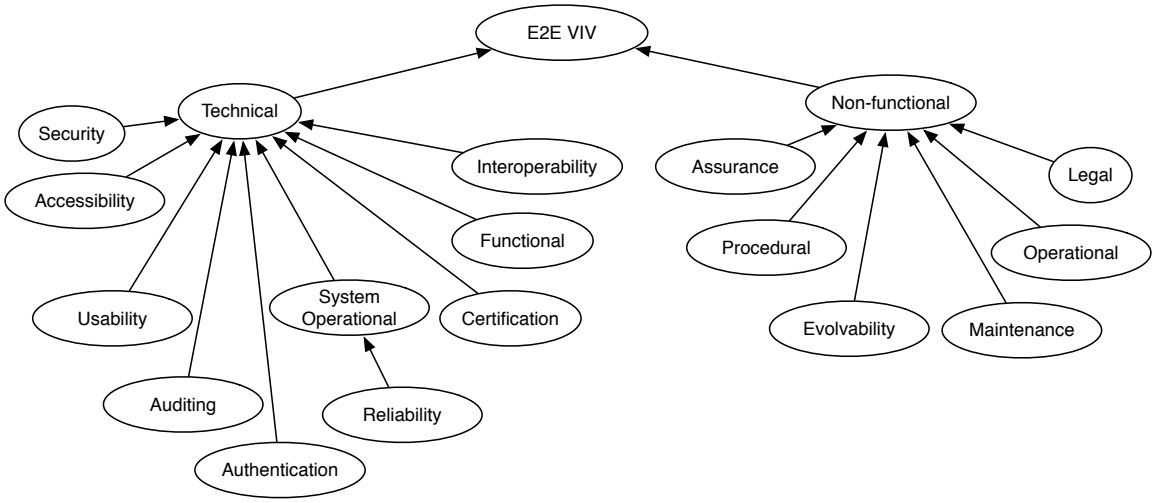

Figure 5.1: The hierarchy of requirements for E2E VIV systems.

Maintaining voter anonymity is critical, so it must be impossible after the election to reconstruct a link between a cast ballot and any identifying information about the voter who cast it. However, in systems that support the casting of multiple ballots, it is important to maintain links between voters and their ballots *during* the election to ensure that later ballots replace the correct earlier ballots. To balance these concerns, any link between a ballot and the voter who cast it must be irrevocably broken once it is conclusively determined that the ballot will be counted toward the final tally.

Finally, because the voter should be able to focus on the voting process without undue distractions or external influences, the voting system must not display or permit the display of any advertising or commercial logos during a voting session; the exception to this rule is that an election jurisdiction may display its own logo to the voter during the voting process. Along the same lines, the voting system must not display any links to other Internet sites outside of the voting system, except to provide help with the actual mechanics of voting.

5.1.2 Usability

The usability of an E2E VIV system is critical to its successful adoption and use. Since the user experience is so important, many of the requirements of the system have some relation to usability even though they may be categorized under other headings. There are, however, two requirements that are exclusively related to the usability of the system with respect to vote casting and one general usability requirement that applies to the system as a whole.

The first vote casting requirement is that, if a voter receives a final vote confirmation (e.g., "Thank you for voting!" or a similar notice) from the system, she can be certain that her ballot was recorded correctly. This is the usability counterpart to the functional requirement that ballot records and voter records must be maintained correctly even in the event of server failures.

The second vote casting requirement is that, if a voter is uncertain whether or not her ballot was recorded (e.g., she clicked a "submit" button but never got a response from the system), she must be free to attempt to vote again.

Finally, usability testing must be performed on any E2E VIV system before it is deployed. The reports of the usability testing must be made public, and the system must achieve satisfactory test results before being deployed in a real election.

5.1.3 Accessibility

Accessibility—the property of being usable by and useful to the disabled—is one of the main goals of an E2E VIV system. It is closely related to usability, but there are several requirements associated specifically with accessibility that go beyond typical usability requirements.

Users must be involved in the design of the system to identify accessibility constraints at each stage of the development process. Consideration must be given to the system's compatibility with existing technologies designed to help disabled individuals; for example, the system should be developed in a way that allows assistive input devices such as switches, eye trackers and screen readers to be used in addition to keyboards, mice and touchscreens. Similarly, the system's presentation of voting options should be optimized to voters' needs by providing alternative display fonts, audio representations, braille representations, and other representations as appropriate.

All possible measures must be taken to ensure that the system can be used by all voters and, if that is not possible in all circumstances, to provide access to alternative methods of voting for those voters who cannot use the system.

Finally, accessibility testing must be performed in addition to the previously-mentioned mandatory usability testing. The reports of the accessibility testing must be made public, and the system must achieve satisfactory test results before being deployed in a real election.

5.1.4 Security and Authentication

Security and authentication are closely related and together represent the broadest set of technical requirements, consisting of both requirements on the E2E VIV system itself (data storage, communications, etc.) and requirements on the voting and counting processes enabled by the system (voter authorization, voter privacy, tally accuracy, etc.).

It is crucial that data integrity be ensured throughout the system. Therefore, measures must be taken to ensure that no data can be permanently lost in the event of a breakdown or fault affecting the system; that the system maintains the integrity of the voters' register, lists of candidates, ballot information, cast ballots, and other critical information, in addition to authenticating the original source(s) of that information and tracking provenance where appropriate; that all data communications within the system have associated integrity checks; that system equipment under the control of the electoral authority is protected against influences that could modify the election results; and that the integrity of the election results does not depend in any way upon the security of system equipment not under control of the electoral authority. The system must perform regular "health checks" to ensure that data integrity has been maintained, that all its components are operating in accordance with their specifications, and that all system services are available.

Accurate timing information is critical to security, both in terms of providing evidence of compliance with applicable regulations and in terms of detecting attacks on and potential breaches of the system. The system must therefore maintain reliable synchronized time sources, with sufficient accuracy to maintain timing data for audit trails, election observation data, and time limits for various aspects of the election process. It must be possible to determine, using the timing information stored by the system, whether nominations (and, if required, acceptance thereof by the candidate or electoral authority), voter registration, and vote casting have occurred within the prescribed time limits for those actions.

Authentication and authorization are also important aspects of security. The system must ensure that each individual can be identified uniquely, so that there is no possibility of mistaking one individual for another. The system must also maintain the privacy of individuals, by ensuring that all personally identifiable data is kept confidential as far as is allowed by the legal requirements of the electoral jurisdiction. The system must allow access to each of its services only to authorized users; for example, only individuals who represent the electoral authority may be allowed to load ballot information into the system.

The authentication mechanisms used to gain access to the system must, as far as possible, protect authentication secrets (passwords, one-time access codes, biometrics, etc.) so that unauthorized entities cannot acquire them. Authentication to the system may not be carried out through third parties; that is, existing online accounts such as those at Facebook, Google and Twitter may not be used as authentication mechanisms. The security of the authentication mechanism must not be affected by any potential breach of any public or commercial database (e.g., a credit card database, the Social

Security database), and it should not be possible for an attacker to impersonate a voter even if the entire database used for authentication in the system is compromised. Individual authentication secrets themselves must be changeable or revokable at any time, at the behest of either the individual or election officials, and must be changed for all individuals at least once in every election cycle.

With respect to the actual voting process, only eligible voters may be allowed to cast ballots and the system must ensure that only the appropriate number of ballots is cast by each voter. It must be possible for a voter to verify that the system has presented her with an authentic ballot and, in the case of remote voting, that she has a secure connection to an official server.

The privacy of the vote must be preserved end-to-end to the maximum extent possible, and individual voters may not waive the privacy of their votes. In the case of remote voting, vote privacy must be preserved even in the presence of arbitrary malicious code on the voter's computer (corrupted client software, key logging software or devices, etc.). Any client software used in remote voting must not send data to any Internet host except those associated with the E2E VIV system or provide any information to third parties (e.g., Facebook, Twitter, etc.) regarding the act of voting. Any residual information that could be used to discover a voter's choices must be destroyed after a ballot has been cast; if a voter uses a computer outside the control of the electoral authority to cast her vote, she must be provided with instructions for destroying any such information on that computer.

With respect to vote counting, the system must accurately count the votes and the counting process must be reproducible. The system must also maintain the availability and integrity of all information used to generate the final tally and all information regarding the counting process itself for as long as required. Vote tabulation must be *software independent*; it must be possible to reconstruct a correct tally from some record even if the election system software is compromised.

Finally, it is expected that a deployed E2E VIV system will be an attractive target for highly-capable adversaries that wish to influence election results or to disrupt election processes. With this in mind, the system must be designed and tested assuming that an adversary has a budget of US$10 per voter per election that can be applied toward any critical subset of votes or voters of their choosing; thus, an E2E VIV system for use in a U.S. presidential election would need to be designed and tested assuming that an adversary has a budget of approximately US$1,300,000,000.

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

5.1.5 Auditing

The ability to perform comprehensive audits of system activity is one of the important distinguishing aspects of an E2E VIV system as compared to other voting systems; as a result, there are several system requirements related specifically to auditing, in addition to those security requirements (such as the tracking of accurate timing information) that touch on auditing.

First, the audit system must be designed and implemented as part of the E2E VIV system from the beginning; it cannot be added as an afterthought to an existing system. Audit and monitoring facilities must be integrated into all levels of the system, from low-level communications among individual computers to high-level interactions with election officials. The system must keep audit logs of all activity relevant to the conduct and outcome of the election, and these logs must be unmodifiable once they are written and as complete as possible without violating voter privacy.

The audit system must actively report on potential issues and threats, rather than merely serving as a passive repository of system logs. It must record at least the following events and actions with accurate timing information: all voting-related information, including the number of eligible voters and votes cast, the number of invalid votes, count and recount results, etc.; any detected attacks on the operation of the system or its communication infrastructure; and any system failures, malfunctions, or other detected threats to proper system operation. It must provide sufficient information to election observers in real time, and after the election's conclusion, to verify that the election is carried out in accordance with applicable law.

The audit system must also be able to cross-check and verify the correct operation of the voting system and the accuracy of the election results, to detect voter fraud, and to prove that all counted votes are legitimate and that all ballots have been counted. In situations where the system cannot verify the legitimacy of all the votes, it must be capable of giving an upper bound on the number of affected ballots. If a tradeoff must be made between maintaining voter privacy and identifying the perpetrators of fraud, the system must resolve that tradeoff in favor of voter privacy.

In order for an E2E VIV system to be trusted, its auditability must extend to its own source code as well as the activities it performs during an election. Therefore, the E2E VIV system software, including any official monitoring and auditing applications, must be published in source form along with documentation, instructions for building and running, and a digital signature as a proof of authenticity.

5.1.6 System Operational

System operational requirements ensure that the system is configured, updated, and run in a transparent, accountable way that allows for the other requirements to be fulfilled. One important such requirement is that there must be official published manifests of the system used to run any election, indicating details of the software and versions used, dates of installation, and brief descriptions of their functionality. Both public and private manifests must be maintained; these should be identical, except that details about software used solely to protect the system against attacks may be omitted from the public manifest for security reasons. Well-defined procedures must exist for both updating the manifests to reflect changes to the installed software and checking the installed software against the manifests to detect tampering.

Before every election period, all equipment (including all software) must be checked and approved in accordance with procedures devised by the electoral authority. This check must include a check of the software against the manifests, as well as any necessary tests to establish that the system complies with its technical specification.

During an election period, key equipment must be located in a guarded, secure area at all times. There must be a contingency plan for system failures including provisions for backup and failover systems, which must conform to the same standards and requirements as the systems they replace. In addition, sufficient arrangements for data backup must be in place, continuously monitored, and always available during the election; election staff must be ready to intervene rapidly, according to a procedure established by the electoral authority, in the event of incidents during an election. Individuals responsible for the voting equipment must follow established procedures to ensure that the equipment and its use satisfy requirements.

To ensure accountability on the part of the electoral authority and election system vendors, a report containing every software manifest change and every violation of data security, system security, physical security or control procedures must be prepared and made public by the electoral authority within a reasonable amount of time after every election.

5.1.7 Reliability

In order to be successfully used to conduct elections, an E2E VIV system must satisfy strict reliability requirements with respect to both its behavior under normal conditions and its behavior while under attack.

In general, the back-end (i.e., non-voter-facing) components of the system must have a proven mean time before failure (MTBF) of at least one week under constant peak expected load; that is, it must have been shown in multiple actual tests of mock elections to run continuously for at least a week at the highest expected voter participation rate. The one week MTBF requirement applies only during normal operation, not while the system is under attack.

In addition to the MTBF requirement, the system must also exhibit 99.9% uptime during the election period, and must be able to recover from any failure other than a regional natural disaster or malicious attack in less than 10 minutes. This must be demonstrated by inducing failures in actual mock election situations, e.g., by unexpectedly unplugging servers or disconnecting storage devices. Redundant failover components must be in place for all critical components of the system in order to ensure the 10 minute maximum recovery time.

An E2E VIV system is likely to be a tempting target for distributed denial of service (DDoS) attacks; it must be able to continue correct operation during a sustained DDoS attack at a specified level on any combination of its back-end components with no more than a specified acceptable degradation of response time to voters during the attack. The specified attack level and acceptable degradation of response time will vary among election types; for example, a system running a national election must be able to resist a significantly higher level of attack than a system running a county election. Our initial suggestions for the thresholds for a national election are that the system must continue operating correctly under a DDoS attack at a level of 100 gigabits per second, with no more than a 15 second degradation of response time.

The ability of the system to survive DDoS attacks and continue operation while fulfilling the response time requirements must be demonstrated in the actual network configuration to be used during the election, and the required thresholds for these values should be re-evaluated every election cycle to keep pace with advancement in attack technology.

5.1.8 Interoperability

E2E VIV systems must use open, rather than proprietary, data and communication standards for interoperability among their various components and services. Whenever possible, the Election Markup Language (EML) or a similar standard ratified by an international standards body should be used for data interchange and configuration within the system. The standards used within the system should allow for localization of election data in situations where such localization is required.

The log data for the system, and documentation describing its meaning and format, must be available for public download so that anybody can download, inspect, and publish concerns based on the system logs.

5.1.9 Certification

In order to provide sufficient evidence for certification of an E2E VIV system, each functional requirement must have an associated set of automated tests that demonstrate its fulfillment. These tests must be runnable on demand, and their results should be unambiguous and easily understandable.

In addition, the election protocol implemented by the system (communication, cryptographic, etc.) must have associated formal proofs of correctness and security.

5.2 Non-functional Requirements

There are five categories of non-functional requirements for E2E VIV systems: operational, procedural, legal, assurance, and maintenance/evolvability.

5.2.1 Operational

The operational requirements on E2E VIV systems deal with several distinct issues including election and registration timing, voter registration, candidate nominations and lists, receipt freedom, voter assistance, and the handling of hardware and software platform issues and election integrity violations.

Voters must be informed, in clear and simple language, of how electronic voting will be organized and what steps a voter will need to take in order to participate and vote electronically. Support and guidance with respect to voting procedures must be available to all voters. In the case of remote voting, such support and guidance must be available through a different, widely-available communication channel (such as a dedicated phone number) in addition to being available via the Internet. Voters must receive clear guidance about exactly what client configurations (i.e., hardware platforms, operating systems, browsers, browser plugins, other applications, and versions thereof) are required by or

supported by the E2E VIV system, and what common components, plugins, or other software (e.g., pop-up blockers, script blockers) may interfere with voting. In addition, voters must receive clear guidance about configuration choices they can make to more strongly protect their privacy; for example, disabling cookies and browser history logging, running privacy-protecting browser plugins, voting from temporary virtual machines, logging out of social networks, disabling non-election-related Internet communications, etc.

In any election carried out using an E2E VIV system, the relevant jurisdiction's legal provisions must provide for clear timetables concerning all stages of the election. The period during which a vote may be cast electronically must not begin before the public is notified of the election; in particular, with respect to jurisdictions that allow remote electronic voting, the voting period must be defined and made known to the public well in advance of its start. In jurisdictions where remote voting takes place concurrently with voting at supervised polling stations, the time periods for remote and supervised voting need not be identical; however, remote voting should not be allowed after the period for supervised voting has ended.

An E2E VIV system must have a publicly accessible voters' register that is regularly updated. Each voter must be able to check, at a minimum, that her information as recorded on the register is accurate, and must be able to request corrections of any inaccurate information. In jurisdictions where remote electronic voting takes place concurrently with voting at supervised polling stations, the system must be designed in a way such that it prevents any voter from voting more than once.

On any electronic ballot, all voting options must be presented equally; that is, there must be no distinguishing fonts, sizes, styles, or other embellishments that could cause one or more of the voting options to be perceived by a voter as "preferred". The ballot must be free of any information about the voting options—biographical information about candidates, interpretations of and statements about ballot initiatives, etc.—other than information strictly required for casting the vote or required by law to be on the ballot (for example, candidate party affiliation is often required to appear). The system must also avoid displaying any messages that may influence voters' choices. Additional information about voting options might be made available from an electronic voting site as part of an E2E VIV system, separate from the actual electronic ballot; if so, such information must be presented without bias.

E2E VIV systems are likely to be made available for testing by voters and election officials, both before and during elections. They must therefore indicate clearly, before the final casting of any ballot, whether the ballot is being cast in a real election or as part of a test. In the case of a test that occurs simultaneously with a real election, individuals casting test ballots should subsequently be directed to the appropriate voting channel for casting real ballots.

E2E VIV systems must exhibit receipt freedom (mentioned previously in the technical requirements); that is, they must not enable the voter to possess a proof of the choices they have made in a cast vote. In a supervised environment, voting information should disappear from the display (visual, audio or tactile, depending on accessibility requirements) used by the voter to cast the vote as soon as the vote has been cast. When a paper proof of an electronic vote is provided to the voter at a polling station, the voter must not be allowed to show it to any other person or to remove it from the polling station.

With respect to counting the votes, an E2E VIV system must not allow the disclosure of any vote counts until after the system has stopped accepting electronic ballots. Tally information must not be disclosed to the public until after the end of the voting period (including all polling station voting). Any decoding required for the counting of the votes shall be carried out as soon as practicable after the end of the voting period; representatives of the electoral authority must be able to participate in, and observers must be able to observe, the counting process. A record of the counting process must be kept, including timing information and identifying information for all persons involved in the counting process. In the event of any irregularity affecting the integrity of votes, it must be recorded that the affected votes had their integrity violated; the effect of such integrity violations on the election results will vary based on the legal provisions of the involved jurisdictions.

Finally, any deployed E2E VIV system must function correctly as an open system, where large parts (specifically, any remote client hardware and software) are unknown, unsecured, uncertified, and completely out of the control of election officials. The system must be auditable to the extent possible given this requirement, and the conclusions drawn from the audit process should be applied in future elections.

5.2.2 Procedural

Successful deployment of E2E VIV systems requires certain procedures to be followed with respect to their provisioning, certification, maintenance, availability, and use. Because such systems are critical pieces of public infrastructure, information about their functioning must be publicly available and information about the specific components of a system must be disclosed, at least to the relevant electoral authority, as required for verification and certification purposes. Before any such system is introduced, at appropriate intervals after its introduction, and in particular when any changes are made to the system, an independent body appointed by the electoral authority must verify that the system is working correctly and that all necessary security measures have been taken.

After introducing a system, the electoral authority must take steps to ensure that voters undesrtand its use and have confidence in the system; these may include outreach, practice elections, and any other measures the electoral authority sees fit. In particular, voters must be given an opportunity to practice any new electronic ballot casting method before, and separately from, the casting of an electronic ballot during a real election.

The electoral authority must take steps to ensure the reliability and security of the E2E VIV system; for example, guarding equipment, providing suitable reliable power supplies, etc. All possible steps should be taken to avoid the possibility of fraud or unauthorized intervention during the voting process, and the electoral authority must satisfy itself that the E2E VIV system is genuine and operates correctly before using it to conduct a real election.

Only individuals appointed by the electoral authority should have access to the central infrastructure, the servers, and the election data, and clear rules should be established for such appointments. Critical technical activities must be carried out by teams of at least two people, and the composition of such teams must be regularly changed. As far as possible, critical technical activities should take place outside of election periods.

Observers must be allowed to be present, to the extent permitted by law, to observe and comment on the conduct and establishment of the results of any election conducted using an E2E VIV system. During an election period, any authorized intervention affecting the system must be carried out by a team of at least two people, be the subject of a written report, and be monitored by representatives of the election authority and election observers.

The system must maintain the availability, integrity, and confidentiality of the votes. It must also keep the votes sealed until the counting process begins. Any votes stored or communicated outside controlled environments must be encrypted. Recounts must be possible, and any features of the system that may influence the correctness of the result must be verifiable. The system must also support partial or complete re-runs of elections.

Finally, there must be clear technical and legal procedures to be followed in the event that voters can prove that their votes were not received accurately or counted, or in the event that the official election verification application does not verify that the results of the Internet portion of the election are correct.

5.2.3 Legal

Legal requirements arise primarily from the application of existing law to E2E VIV systems. These include requirements on accessibility and availability; on the counting of votes, number of votes per voter, and anonymity of votes; and on restrictions with respect to reverse engineering or testing of E2E VIV systems.

To comply with accessibility and availability requirements, the voting interface of an E2E VIV system must be understandable and easily usable, and registration requirements for electronic voting must not pose an impediment to voter participation. E2E VIV systems should be designed, as far as is practicable, to maximize the opportunities they provide for the disabled. Unless remote electronic voting channels are universally accessible, they must be used only as an additional and optional means of voting beyond polling places or more traditional remote voting methods.

The E2E VIV system must insure that at most one electronic vote from each voter is included in the final tally, that every vote cast electronically is counted, and that each vote cast electronically is counted only once. In jurisdictions where electronic and traditional voting channels are used in the same election, there must be a secure and reliable method to aggregate all votes, prevent multiple votes by the same voter from being counted, and calculate correct results.

The way in which voters are guided through the process of electronic voting should be designed to prevent their voting precipitately or without reflection. Voters must be able to alter their choices at any point during an electronic voting process before casting their vote, or to stop the voting process, without their previous choices being recorded or made available to any other person under any circumstances. The electronic voting system must not permit any manipulative influence to be exercised over the voter during the voting process, must provide the voter with a means of participating in the election without exercising a preference (e.g., by casting a blank ballot), must indicate clearly to the voter when the voting procedure has been completed, and must preserve voter anonymity.

There must be no legal impediments to interested parties who want to study the E2E VIV system. In particular, no nondisclosure agreement or contract of any kind may be required for such download and study, or for building, testing and publishing test results for the E2E VIV system.

5.2.4 Assurance

There are several assurance requirements with respect to the implementation, documentation, and licensing of E2E VIV systems. First, client side software—that is, any software that is expected to be used on a system serving as a voting terminal, whether a supervised machine at a polling place or an unsupervised machine belonging to a voter—must be free of known bugs on a wide range of platform and software stack combinations. As previously discussed in Section 5.2.1, the specific supported platform and software stack combinations for the software must be clearly conveyed to voters. The system must exhibit strong security with respect to voter authentication, such that there is no way to automate forging or invalidation of voter authentication credentials without compromising the cryptographic protocols or secrets used in the system.

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. As the system changes, all associated documentation must be kept up to date, and no new version of an E2E VIV system should be certified until it has up-to-date documentation.

The source code, build scripts, issue tracking system, security features, and related development information for the entire Internet voting system—all versions, for all supported platforms—should be made publicly available for free download and inspection, under a license that permits anyone to download, build, instrument, and test the system.

5.2.5 Maintenance and Evolvability

Maintenance and evolvability requirements are closely related, and essentially stipulate that an electoral authority, or any entity engaged by an electoral authority, must be able to change an E2E VIV system in response to changes in the legal or technical environment in which it operates.

The electoral authority must have the right and the ability to update the election system to conform to changes in applicable law, available technology, or threats to system integrity independent of the original vendors of the system. The electoral authority must also have the right and ability to patch election systems to correct flaws discovered in the algorithms, implementation, or deployment, subject to the documentation update requirement described above and the procedural requirement that the system must be re-verified for correct operation before being used to conduct a real election.