Carnegie Mellon University
HeinzCollege

Comparative Analysis of Potential

E2E VIV Systems

OVERSEAS VOTE
FOUNDATION

Part I of the Overseas Vote Foundation's
End-To-End Verifiable Internet Voting Project

Draft **Final Report**

May 2, 2014

Capstone Team

Bingbing Hou Γ Sunny Sharma

Kahlil Wallace Γ Candice Hoke Γ Travis Wright

Faculty Advisor

Randy Trzeciak

Introduction to Draft Report

This draft Capstone report presents research on 16 voting systems that appeared to be contenders for consideration as E2EV systems.

We began our research by seeking to develop a working definition of an E2EV voting system that commanded broad support among the esteemed scientists and subject matter experts that OVF convened. After confirming that threshold conclusion, we sought to research and evaluate all systems by those criteria.

Limitations: The Capstone team was not charged with conducting any independent verification of the representations developers and vendors made regarding the technical and operational facts regarding their systems. Hence, if the documentation did not accurately state technical facts, our report repeats those errors. Because none of these systems have been submitted for testing under the EAC-VVSG standards, we did not have access to test reports or plans, and generally were not able to access any other source of independent testing or documentation. More concretely, if a system's documentation or developers stated they used "the most secure encryption protocols yet available" and noted reported that the system used DES, we reported only the specific encryption standard used but excluded the marketing claim that also incorporated a false proposition.

Ultimately, our analysis of system features we found that only 3 systems could meet the E2EV definition on the basis of the materials we could access. We then augmented research on new systems currently under development that held the promise of meeting E2EV criteria.

Although we initially reached out to proprietary vendors, we did not have the bandwidth for extended negotiations over what types of documentation they might be willing to provide. Given that vendors often seek for researchers to sign a nondisclosure agreement and that Heinz Capstone rules generally proscribe such covenants, we chose to follow Ron Rivest's advice and use only publicly available documentation.

We sincerely request frank feedback and recommended improvements to this draft report before we finalize it.

Table of Contents

Group I Systems

Remotegrity

Introduction

During the mid-2000s, the remote voting system **Remotegrity** was proposed and developed by Filip Zagorski, joined by a team of other noted cryptographers that included Poorvi Vora, Richard T. Carback, David Chaum, Jeremy Clark & Aleksander Essex. [R1]. Remotegrity is an end-to-end verifiable (E2EV) absentee voting system, which has been architected to work in concert with an in-person/precinct voting system called ***Scantegrity*** (a paper-based system). Remotegrity adapts the "code-voting[1]" approach and features found in the "mother-system" Scantegrity. It thereby seeks to protect voter privacy, resiliency against any malware-induced software modifications, election official or intruder manipulations of vote tallies, and other potential injuries to election integrity. The most recent use of Remotegrity occurred in Takoma Park, Maryland, in 2009, where election officials deployed Remotegrity as a component of its trial of both Scantegrity/Remotegrity and ***ranked-choice voting***[2] methods. In this report we have reviewed the version of Remotegrity used in the 2009 Takoma Park local election. Our analysis is based on the publicly available research papers and interviews with the individual architects and developers.

1. Core Architecture & Operation

1.1 Basic Architecture & Design

Remotegrity uses both the online component as well as the paper component from ***Scantegrity.*** Paper ballots are printed along with an additional feature called the 'Authorization card'. The Authorization card contains codes which are hidden under a scratch off and which are used in casting the vote ('Auth Code') and finalizing the casted vote ('Lock Code'). These two printed components are sent to the registered voters via any postal service and the online component includes voters accessing the voting site, casting the vote, checking their vote and finally viewing the results on a publicly accessible Bulletin Board (which is another website).

Remotegrity is developed in Java. The databases (for example: MySQL) can be hosted on a cloud infrastructure. The system requires a separate offline server that is not internet-facing to check the validity of the voters' submitted vote & authorization codes. This server is dedicated to maintaining all the cryptographic keys and validation signatures. Remotegrity developers architected the system for high security and data integrity and tested it for security gaps prior to deployment in Takoma Park.

[1] Code voting helps in achieving privacy by replacing all the elements on a ballot by codes which are cryptographically generated

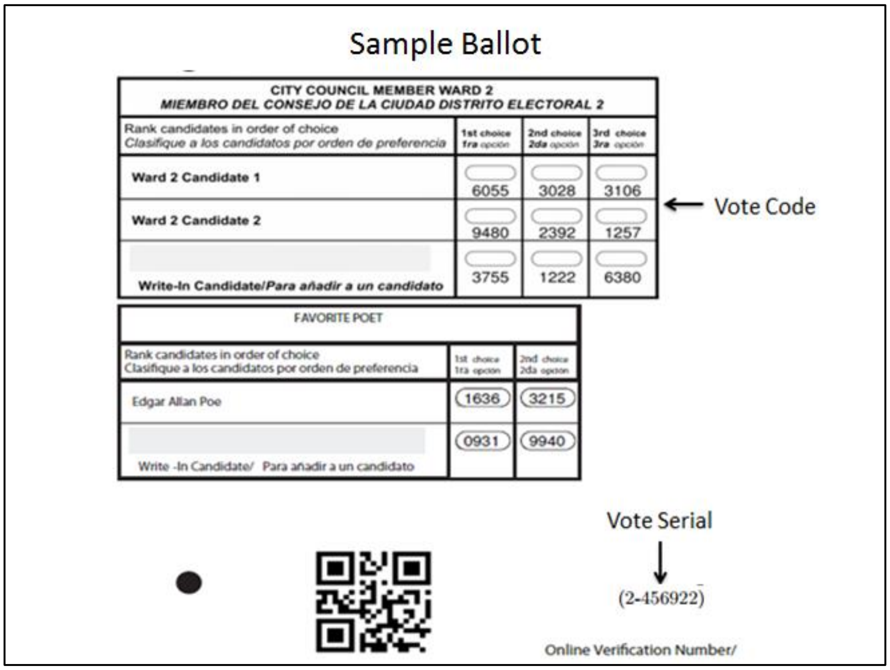
[2] "Ranked-choice voting" (also called preferential or "instant run-off voting" (IRV) requires voters to rank their choices among the available candidates. While IRV election can be structured with different rules (for instance, at least two distinct types of IRV structures can be created, including e.g., directing voters to "rank your top three choices of candidates by placing a '1' indicating your top choice, and '3' your third choice among the field of 8 candidates," or "Rank each of the 8 candidates in the order of your preference, giving a '1' to your top choice candidate and an '8' to your least preferred candidate." The virtues and evils of IRV are well beyond the scope of this Report. Suffice it to say that IRV presents substantial voter education hurdles, and that the test-running of Remotegrity in concert with IRV eliminates the ability to draw any sound conclusions about the usability or deficits in either innovation.

Remotegrity is designed to ensure that voters will receive unique codes for the same candidate.[3] This ensures that all the relation between the codes and the voter is also retained by the election official to verify the voter in case of any dispute. These codes are cryptographically calculated using the keys the election officials generate via automated processes.

Remotegrity's use of cryptography differs from the ***Helios*** voting system in one major way: Remotegrity encrypts this encryption happens before the voting takes place. Helios encrypts the codes are implemented after the vote has been cast, in.

1.2 Voting Process

Printing Ballots: Before ballots are printed the unique codes for every candidate are calculated along with the Auth and Lock codes for all voters. These cryptographic values and their relation to candidates and voters are generated and stored on an offline validation server. The ballot paper and the authorization card also contain a 'Vote Serial' and 'Ack Code' respectively. These are used to confirm the validity of the codes entered came from a particular ballot and an authorization card. The ballots and the authorization cards are printed and mailed to all the voters. The sample ballot and the sample authorization card are shown in Fig 1 and Fig 2 below.


Sample Ballot
Vote Code
Vote Serial

CITY COUNCIL MEMBER WARD 2 *MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 2*			
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
Ward 2 Candidate 1	○ 6055	○ 3028	○ 3106
Ward 2 Candidate 2	○ 9480	○ 2392	○ 1257
Write-In Candidate/*Para añadir a un candidato*	○ 3755	○ 1222	○ 6380

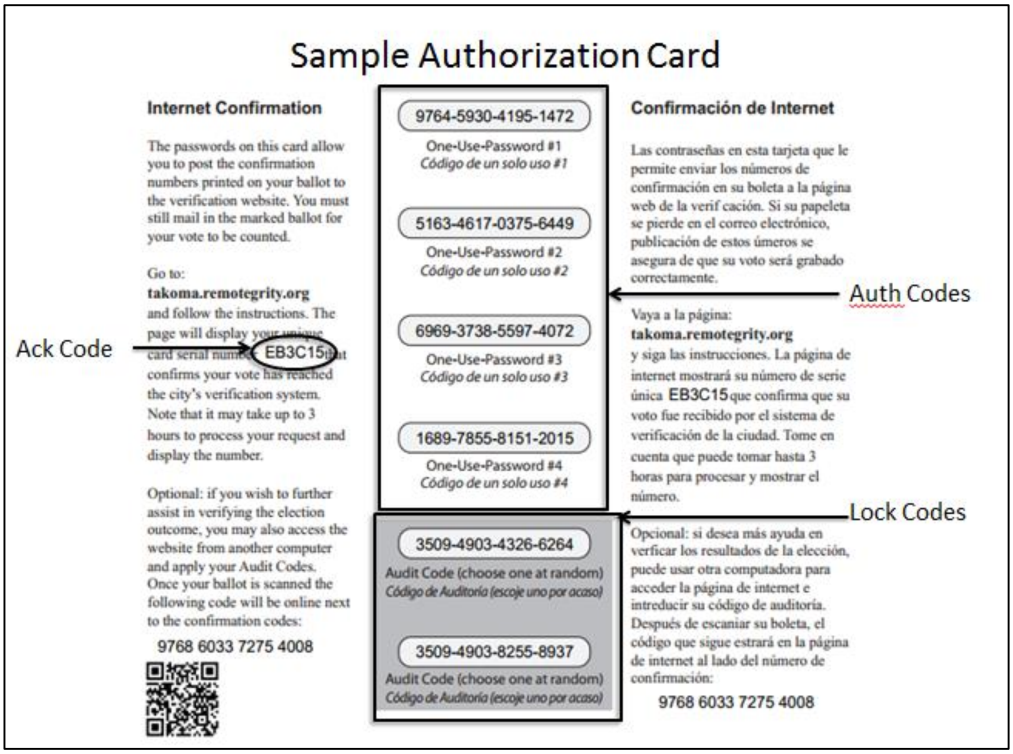
FAVORITE POET		
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1st choice 1ra opcion	2nd choice 2da opcion
Edgar Allan Poe	1636	3215
Write -In Candidate/ Para añadir a un candidato	0931	9940

(2-456922)

Online Verification Number/

Fig. 1 Sample Ballot

[3] The system utilizes distributed key generators & pseudo-random number generators for generating the codes that are printed on the ballots and authorization cards.



Sample Authorization Card

Internet Confirmation

The passwords on this card allow you to post the confirmation numbers printed on your ballot to the verification website. You must still mail in the marked ballot for your vote to be counted.

Go to:
takoma.remotegrity.org
and follow the instructions. The page will display your unique card serial number EB3C15 that confirms your vote has reached the city's verification system. Note that it may take up to 3 hours to process your request and display the number.

Optional: if you wish to further assist in verifying the election outcome, you may also access the website from another computer and apply your Audit Codes. Once your ballot is scanned the following code will be online next to the confirmation codes:

9768 6033 7275 4008

9764-5930-4195-1472
One-Use-Password #1
Código de un solo uso #1

5163-4617-0375-6449
One-Use-Password #2
Código de un solo uso #2

6969-3738-5597-4072
One-Use-Password #3
Código de un solo uso #3

1689-7855-8151-2015
One-Use-Password #4
Código de un solo uso #4

3509-4903-4326-6264
Audit Code (choose one at random)
Código de Auditoría (escoje uno por acaso)

3509-4903-8255-8937
Audit Code (choose one at random)
Código de Auditoría (escoje uno por acaso)

Confirmación de Internet

Las contraseñas en esta tarjeta que le permite enviar los números de confirmación en su boleta a la página web de la verif cación. Si su papeleta se pierde en el correo electrónico, publicación de estos úmeros se asegura de que su voto será grabado correctamente.

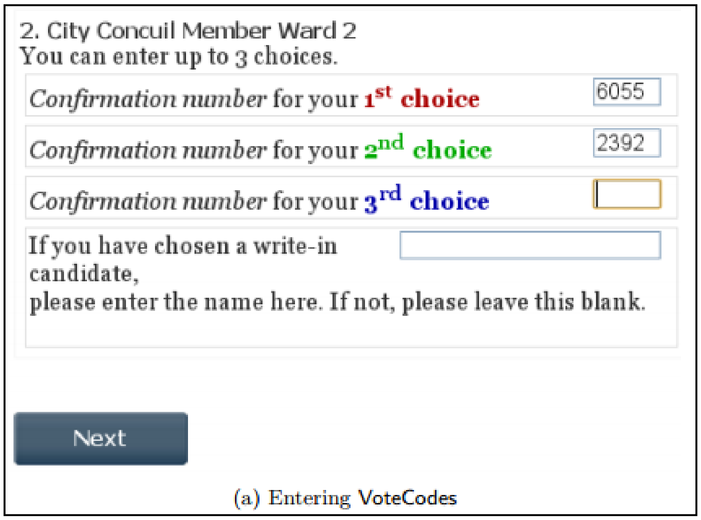
Vaya a la página:
takoma.remotegrity.org
y siga las instrucciones. La página de internet mostrará su número de serie única EB3C15 que confirma que su voto fue recibido por el sistema de verificación de la ciudad. Tome en cuenta que puede tomar hasta 3 horas para procesar y mostrar el número.

Opcional: si desea más ayuda en verficar los resultados de la elección, puede usar otra computadora para acceder la página de internet e intreducir su código de auditoría. Después de escaniar su boleta, el código que sigue estrará en la página de internet al lado del número de confirmación:

9768 6033 7275 4008

Fig. 2 Sample Authorization Card

Ballot casting: The voters will use the 'Vote Code' as shown in Fig. 1 of their preferred candidate and enter it on the voting portal. Upon entering their choice, the voter is asked to enter and 'Auth Code', which is under a scratch off on the authorization card. This 'Auth Code' is a one-time password used to validate the voter. There are 4 Auth codes given to a voter under a scratch off, which are helpful in case the voter needs to change his choice or in case there is a dispute over the values entered. Once the values are entered, the voter is asked to wait for some time until the election official verifies the codes entered by the voter are verified. The election official upon verifying the values signs the code entries and displays it back to the user. Upon verification the voter is shown his choice along with the Vote Serial and the Ack Code. If the voter is satisfied, he/she has to scratch off one of the 'Lock codes' and use the value to finalize/freeze the vote. Once the 'Lock Code' is used the vote cannot be changed. Fig 3 shows Vote codes being entered. Fig 4 shows Auth Code being entered. Fig 5 shows the verification back to the voter along with the Auth Code-EB3C15



2. City Concuil Member Ward 2
You can enter up to 3 choices.

Confirmation number for your 1st **choice** 6055

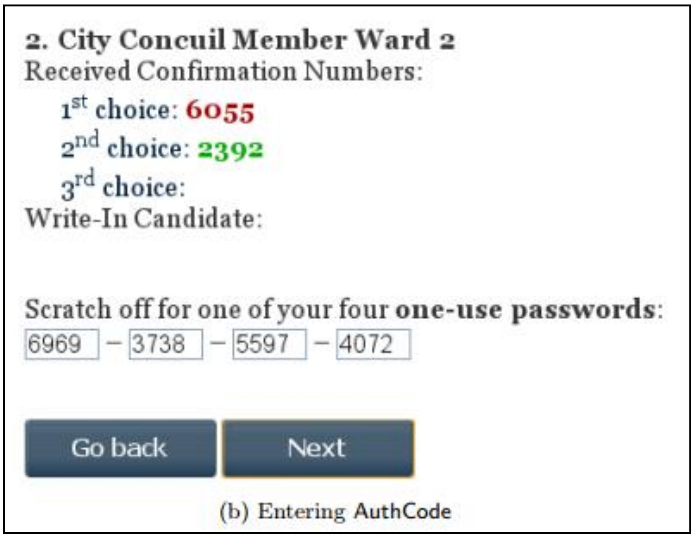
Confirmation number for your 2nd **choice** 2392

Confirmation number for your 3rd **choice**

If you have chosen a write-in candidate,
please enter the name here. If not, please leave this blank.

(a) Entering VoteCodes

Fig. 3 Vote Codes entered – 6055 & 2392

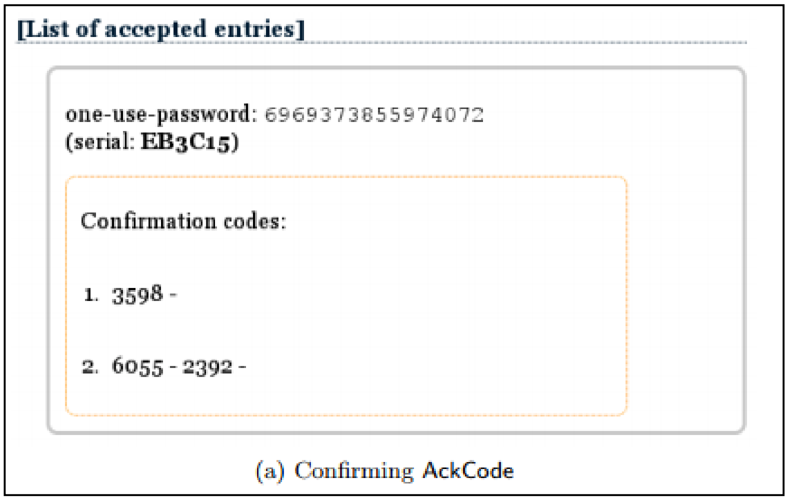


2. City Concuil Member Ward 2
Received Confirmation Numbers:
1st choice: **6055**
2nd choice: **2392**
3rd choice:
Write-In Candidate:

Scratch off for one of your four **one-use passwords**:
6969 – 3738 – 5597 – 4072

(b) Entering AuthCode

Fig. 4 Auth Code entered - 6969-3738-5597-4072



[List of accepted entries]

one-use-password: 6969373855974072
(serial: **EB3C15**)

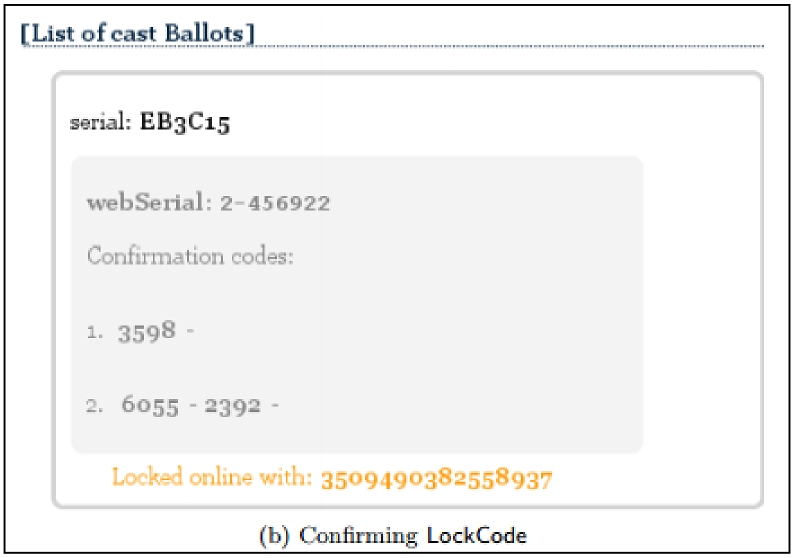
Confirmation codes:

1. 3598 -
2. 6055 - 2392 -

(a) Confirming AckCode

Fig. 5 User shown his/her choice along with Ack & Auth Code on a public Bulletin Board

Results: Once the final tally is done the results are displayed on a publicly accessible bulletin board. For a particular voter, this will show his candidate's 'Vote Code', the 'Vote Serial' of the ballot paper, the 'Auth Code' used, the 'Lock Code' used and the 'Ack code' of the authorization card. Fig 6 shows the final vote as seen by the user post the completion of the tally. Here the voter is shown the Lock code as well as the Vote Serial along with other codes



[List of cast Ballots]

serial: EB3C15

webSerial: 2-456922

Confirmation codes:

1. 3598 -
2. 6055 - 2392 -

Locked online with: 3509490382558937

(b) Confirming LockCode

Fig. 6 Final vote confirming the Lock code & Vote Serial (2-456922)

2. Security

2.1 Security Overview

Remotegrity utilizes the "code-voting" approach and features found in Scantegrity voting system. It thereby seeks to protect voter privacy, resiliency against any malware-induced software modifications, election official or intruder manipulations of vote tallies, and other potential injuries to election integrity. It uses Distributed key generators and pseudo random generators are used to build share secret amongst the election official, which is then used to generate the codes.

2.2 Malware Resiliency

In the voting process the values entered by the voter are the Vote, Auth & Lock codes. The values which are never entered by the voter are Vote Serial and the Ack Code (which are only shown to the user once the vote is casted).

Considering a case where the malware makes changes to the entered Vote code during ballot casting, this will be rejected by the election official while he performs the initial verification, since this vote code will not generate a relation with the corresponding relation to the Vote serial for this particular voter. Also, since the vote codes are generated randomly there is low probability that the malware will be able to guess a correct alternative code for a particular candidate.

Considering the malware is able to guess a valid code for a candidate, it should also know a valid Auth Code for confirming the choice. Since the Auth codes are generated randomly and sufficient in length the malware with high probability will not be able to guess the correct alternative Auth code (which would be still under a scratch off). Any chances of a malware changing the Auth code will also be rejected since this Auth code will not generate the relation with the Ack Code for that particular authorization card for the voter.

2.3 Malfeasance by Election Official and Dispute Resolution

The use of Auth codes and the Lock codes under a scratch off makes sure that there is no malicious activity by an election official. As we mentioned earlier an election official has to sign every entry he/she verifies before posting it on bulletin board, this makes sure that the election official is responsible for the results shown to the voter. Another feature of Remotegrity requires the use of a new Auth code every time an election official signs an entry, thus if an election official alters the values on the bulletin board after the voter submits the vote means that the election official would require a new Auth code or a Lock code which was not scratched off by the voter. This makes it easier to detect any alterations made by an election official and point out the official who signed that entry. These properties of the system also allow in maintaining vote integrity and helps in resolving any disputes.

3. Voter Privacy

Remotegrity utilizes code voting. This is a feature in which the identities of the voter and the candidates are replaced by cryptographically generated codes and the relation/binding between them is retained for verification purpose. In Remotegrity, the candidates are replaced by 'Vote Code' present on the printed ballot and the validity of the voter is verified by the use of the one-time password known as the 'Auth Code'. Every voter gets a generated 'Vote Serial' and 'Ack code' this allows the voter to verify that the choice of the candidate entered by him on the voting system was recorded correctly. Since the final results are displayed publicly as codes entered by the voter, only the voter knows his vote/choice and does not make any sense to anyone else. This feature also makes this system universally verifiable.

Details on ***Auditability***, ***Trust structure*** and other aspects can be found in the System detail table.

4. Infrastructure required

By the election official –

1. Officials who will generate the master secrets for generating the codes
2. Hardware for printing with the capability of having the Auth and Lock codes under a scratch off
3. A web server infrastructure in case standalone hosting is done or a cloud infrastructure can be used

By the voter –

1. A computer or a smart phone with an internet connection.

5. Shortcomings

We have seen so far that the Remotegrity voting system which was used in Takoma Park is an end to end verifiable absentee voting system which is capable of ensuring the integrity of the votes, results, privacy of the voters, resiliency to changes made by malware and an election official, dispute resolution. However, this system does not is not meant to be coercion resistant. Moreover, like any other web facing infrastructure this system by itself is not capable of coping up with any kind of denial of service attack. This risk can however be reduced if the system is deployed on a cloud infrastructure which provides very high percentage of up time. We also did not have any data on the usability aspects of this voting system. It is also yet to be seen how this system can scale up to a larger county or state level election.

References:

[R1] Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System, Filip Zagorski et.al. - https://eprint.iacr.org/2013/214.pdf

[R2] A. Essex, J. Clark, U. Hengartner, and C. Adams. Eperio: Mitigating technical complexity in cryptographic election verification. - https://eprint.iacr.org/2012/178.pdf

[R3] Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy, David Chaum et.al. - https://www.usenix.org/legacy/events/sec10/tech/full_papers/Carback.pdf

[R4] Remotegrity FAQ - http://www.scantegrity.org/wiki/index.php/Remotegrity_Frequently_Asked_Questions#What_can_go_wrong_with_Remotegrity.2C_and_how_will_you_protect_against_it.3F

[R5] Cryptographic Voting Debuts, MITnews, http://web.mit.edu/newsoffice/2009/rivest-voting.html

[R6] Remotegrity Poster - http://zagorski.im.pwr.wroc.pl/papers/Remotegrity-poster.pdf

[R7] Takoma Park Public Bulleting Board - http://takoma.remotegrity.org/BulletinBoardFinal.php

[R8] B. Adida. Helios: web-based open-audit voting. In USENIX Security Symposium- static.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf

System Details -> Remotegrity

I. CORE ARCHITECTURE & OPERATION FEATURES

Issue	Summary Answers
Features of the system; paper, pure electronic, etc?	Remotegrity is online(uses web infrastructure) as well as paper based system
Programming Language(s)	Remotegrity is developed in Java
Encryption Method(s)	Distributed key generators and pseudo random generators are used to build share secret amongst the election official, which is then used to generate the codes
Which of the following stages of the voting process are encrypted? 1) Blank ballots at time of distribution to voter, 2) Voted ballot after ballot selections (votes) are marked, as part of casting, 3) Vote recording at the LEO, 4) Tabulation processes.	All the stages of the voting process are encrypted
Does the VS supply adequate and clear documentation to LEOs to facilitate efficient, accurate set up of an election & operation?	No data available
Does the VS supply dedicated voter education materials (or online tutorials) to introduce the system's operation to voters?	No data available

How scalable is the system? What voting population and expected ballot cast numbers can it accommodate?	In Takoma Park elections, there were 11,000 registered voters. However, Remotegrity claims that it is scalable for larger elections. We at this point are not able to verify this claim.

II. Security Design & Security Testing

Issue:	Summary Answers
Describe the security architecture & design features.	Remotegrity is a E2EV system. It is designed to safeguard, voter privacy, resiliency against any malware-induced software modifications, election official or intruder manipulations of vote tallies. It utilizes 'code voting', which ensures that voter privacy is maintained as well as voting integrity is maintained. This system is also universally verifiable, as the results are shown on public bulletin board and voters can verify if their votes are recorded accurately and counted in the final tally.
Do developers explicitly claim the system programming complied with security best practices? E.g., OWASP Top Ten or other guides? If so, which best practice guides explicitly mentioned in documentation?	We were not able to identify any documentation on Remotegrity which describes this. However, based on the interview with the developer we understand that the system was developed by keeping in mind the OWASP top ten web application vulnerabilities.
What error/anomaly detection and error correction capabilities are built-in?	This system uses code voting and presents the voters with 'Auth Codes' and 'Lock Codes' which are under a scratch off. These codes are used to cast a ballot and finally lock in the ballot respectively. Any changes to the votes on the bulletin board require the use of a new 'Auth code' & 'lock code' along with a digital signature from the election official. If there is any change to the votes, voter can easily detect it as the codes will not match and this change will be attributable to an election official.
How does the voting system provide resistance towards malware at voter/client side?	Since the coded ballots are provided on paper to the voter, the device used by the voter will neither be able to guess the correct codes assigned to a candidate nor the correct Auth & Lock codes.
	Any changes to the votes on the bulletin board require the use of a new 'Auth code' & 'lock code'

How does the voting system provide resistance towards malware at election official/server side?	along with a digital signature from the election official. If there is any change to the votes, voter can easily detect it as the codes will not match and this change will be attributable to an election official.
How does the voting system provide resistance to client/voter side denial of service (DOS) attacks?	Just like any other web based system, this is also susceptible to DOS attacks. This system is not designed to tackle any DOS on the voter side.
How does the voting system provide resistance to election official/server side DOS attacks?	Just like any other web based system, this is also susceptible to DOS attacks. However, this risk can be mitigated by hosting this system on a cloud environment
What methods of resilience against coercion to voters and local election officials are available with this system?	This system does not provide any solution towards coercion
Has there been a network and/or application security assessment by security experts for this system?	Before the Takoma Park election, this system's backend as well the web interface has been tested for security weaknesses by two independent researchers: Marco Ramilli and Marco Prandini
Were the results of the security assessment publically published?	We could not find a complete report on the results of the testing. However, based on [R1] and interview with the developer we understand that there were several issues related to web interface; which were fixed before the election.
Were details for a security patching process provided for this system?	Based on [R1] and interview with the developer we understand that there were several issues related to web interface; which were fixed before the election. However, we could not find any documentation on the patching process.
Does the system provide data redundancy in the case of a disaster?	This system can be hosted on cloud environment and hence can provide redundancy based on the requirements of the election and based on the capabilities of the cloud service provider.

Do the developers/vendor offer recommendations to LEOs re key management? ***If yes,*** do they mention operational processes, privilege/separation of duty, or special equipment/software for key management?	There is no documentation available on the key management practices.
If the LEOs private keys were to be compromised by a hacker or insider in some manner, describe the damage to the integrity/accuracy of the vote totals/results that could be achieved. If unauthorized key access could lead to tampering with vote totals, would that tampering be detectable? If so, what kind of analysis would be required to identify/detect that tampering?	This system uses Distributed key generators and pseudo random generators are used to build share secret amongst the election official, which is then used to generate the codes. By virtue of the cryptography used, any compromise to the integrity of the voting process is detectable. As, any changes to the votes on the bulletin board require the use of a new 'Auth code' & 'lock code' along with a digital signature from the election official. If there is any change to the votes, voter can easily detect it as the codes will not match and this change will be attributable.

III. TRUST STRUCTURE

When this system is deployed, who (and what equipment or processes) must the voter, the general public and election officials, trust to be working correctly – without any additional or independent verification other than what this voting system provides-- that all votes have been recorded, transmitted, tallied and reported accurately?

Issue	**Summary Answers**
Whom (or what equipment & processes) must the voter trust that: • the correct blank ballot is delivered with all races and issues present?	Since the codes on the ballots are printed and sent to the voters before the election, the voter needs to trust the election officials for obtaining the correct ballot with correct codes.
• their choices (candidates and/or issues) are recorded correctly before the marked ballot leaves their device?	Once the voter has the ballot the voter does not need to rely on the device used or even the internet, since the voter is able to verify if the correct choices have been recorded on the bulletin board.
• their ballot as been received by local election office?	The voter does not need to rely on the election officials, since the voter is able to verify if the correct choices have been recorded on the bulletin board.
• that their ballot has been a part of the tabulation?	The voter does not need to rely on the election officials or the system, since the voter is able to verify if the correct choices have been recorded and counted in the final tally on the bulletin board.
• that their ballot choices have been tallied correctly in the total cast ballots results?	The voter does not need to rely on the election officials or the system, since the voter is able to verify if the correct choices have been recorded and counted in the final tally on the bulletin board.
Whom must the local election official trust • that the ballot presents the correct ballot choices for a given voter?	All the ballots recorded are verified to make sure that each ballot has a valid Auth code associated. Any false ballots will be filtered as such ballots will not be able to prove the relation between the candidate codes, vote serial, Auth code.

Whom must voter & general public trust that the votes have been tallied & reported to the public correctly?	The voter does not need to rely on the election officials or the system, since the voter is able to verify if the correct choices have been recorded and counted in the final tally on a publicly verifiable bulletin board.

IV. AUDITABILITY

Issue	Summary Answers
1. What types of protections does the Voting System "**VS**" (or via the operational/managerial election processes it recommends) provide for assuring that the voter's ballot choices are not modified in an undetectable manner? ***Specifically***	See below
a. Does the system produce a voter-verifiable, durable, tamper-evident artifact (abbreviated "**V V-D-TEA**")?[4] ***If yes,*** describe the type of artifact it produces (e.g. physical or digital)?	Yes
b. Can any additions, deletions, or substitutions to the voter's ballot selections (votes) be detected, using the **V V-D-TEA** records?	Yes
c. Can the results of the election contests (races and issues) be reconstructed (recounted) independently of using the voting system's software, simply by using the **V V-D-TEA** records?[5]	Yes
d. Does the system require additional audit checks, for instance by using digital signatures and hashes? ***If yes***, explain what additional integrity checks (at what junctures	All the entries of recorded votes on the bulletin board accompany Ack & Auth codes in addition to being digitally signed by election officials. Any changes to the ballots are detectable by the election official as well as the voter

[4] Noted voting system auditing expert Dr. Phillip Stark recommended this set of attributes that we have abbreviated "V V-D-TEA."

[5] This question asks for whether the system can be described as producing a voting record and potential for election results that are "software independent." *See* Rivest & Stark, and Stark & Wagner (cites)

and for what purposes) have been designed into the system.	
2. Does the voting system support the auditing of:	
a. # of blank ballots sent to voters	Yes
b. # of voted ballots received from voters	Yes
c. Verifiability of votes as recorded?	Yes
d. Verifiability of cast as recorded	Yes
e. Verifiability of tallied as cast	Yes
3. Does the auditability design of the voting system require via hard-coded [nondiscretionary, within range of reasonability] logs of operators' interaction with:	
a. blank ballots generator/database	Yes
b. voted ballots collection system/database	Yes
c. cast ballots storing system/database	Yes
d. cast ballots tallies	Yes
e. cast ballots reports	Yes
f. system failures, malfunctions and other threat or attack on the operation of the voting system, as well as other infrastructure components	Yes
4. Are these audit logs protected from administrative or operator modifications (insider threat)? If yes, explain how.	All the entries of recorded votes on the bulletin board accompany Ack & Auth codes in addition to being digitally signed by election officials. Any changes to the ballots are detectable by the election official as well as the voter
5. Are these audit logs protected against operations (e.g., system crashes) or attacks	All the entries of recorded votes on the bulletin board accompany Ack & Auth codes in addition to being digitally signed by election officials. Any changes to

which could lead to data corruption or loss? If yes, explain how.	the ballots are detectable by the election official as well as the voter
6. Does the audit system maintain voter anonymity at all times? If yes, explain how	Since code voting (Code voting helps in achieving privacy by replacing all the elements on a ballot by codes which are cryptographically generated) is utilized and the threshold shares are spread amongst the election official (which are used to generate the codes), voter anonymity is maintained throughout the voting process.

V. VOTER ANONYMITY

Issues:	Summary Answer
1. Does the voting system maintain voter's anonymity while • Voter is accessing the system to obtain or mark a ballot?	Since code voting (Code voting helps in achieving privacy by replacing all the elements on a ballot by codes which are cryptographically generated) is utilized and the threshold shares are spread amongst the election official (which are used to generate the codes), voter anonymity is maintained throughout the voting process.
• Voter is marking and casting his/her vote?	Yes
• the vote is being recorded at the LEO?	Yes
• the vote is being tallied?	Yes
2. Does the voting system maintain anonymity after the final results are posted?	Yes
3. Can voters/users post feedback or make complaints anonymously?	No. Any dispute resolution complaints will have to be made to the election official
4. Does the system monitor the voter/user while the system is in use?	Refer to Q1
5. Could an adversary track/trace a user and connect the user to a particular cast ballot after compromising the system?	No, considering the encryption system is not compromised

VI. Testing, Certification & Deployments

Issues:	**Summary Answers**
Testing *(exclusive of testing discussed under* **Security** *&* **Usability***)*	
1. Has the system received reliability testing or any other testing specified by the Voluntary Voting System Guidelines (VVSG)?	No
2. If yes, what VVSG-specified testing and with what results?	No
3. Has the system been submitted for certification under the EAC voting system process? If so, provide details of when and with what results.	No
4. Has the system received open-ended vulnerability testing, as recommended by the EAC's Technical Guidelines Development Committee?	No
5. If yes, detail by whom/ when/ where?	No
6. Has the system undergone any other independent testing, not by the internal developers but by a qualified independent organization or set of individuals? If so, describe with dates and published reports.	No
	No

7. Have the developers announced any planned independent testing? If so, when?	
Certifications	
8. Has the system undergone any certification testing? If so, in what State or jurisdiction, and with what results?	No
9. Has the system been certified for use by some States or jurisdictions? If so where?	No
Current or planned deployments?	
Public Government elections? If so, where and dates?	No
Private/ nonprofit/ labor unions, etc. If so, where/when?	No

VII. Usability/ Accessibility

Issues	Summary Answers
Usability: 1. Has a usability study been conducted by qualified usability assessors and published by public or scholarly access?	No Data available
2. If yes, did the study report deficiencies in the system with regard to usability?	No Data available
a. Comprehension & success in marking of ballot?	No Data available
b. Comprehension & success in casting of ballot?	No Data available
c. Comprehension & success in verifying of ballot?	No Data available
3. Did the study report usability deficiencies in the system with regard to election official set up of the election?	No Data available
4. Discuss the quality and completeness of the documentation for LEOs to set up the system, create of ballots and tabulation, voter education, and other aspects.	No Data available
Accessibility: 4. Is the system designed for persons with physical impairments that may affect voting? Specifically	
a. Blind	No Data available
b. Deaf	No Data available
c. Multiple impairments	No Data available
	No Data available

5. Has an accessibility study been conducted by qualified accessibility assessors, published by public or scholarly access? ***If so,*** cite.	

VIII. Infrastructure:

Staffing, Training & Equipment Needed to Conduct Elections Successfully & Securely

Issue	Summary Answers
Equipment needed by Voter to receive, mark & cast ballot	A computer or a smart phone with an internet connection.
Equipment needed by LEO to develop ballots, send to voters, receive marked ballots, & tabulate plus report?	• Officials who will generate the master secrets for generating the codes • Hardware for printing with the capability of having the Auth and Lock codes under a scratch off • A web server infrastructure in case standalone hosting is done or a cloud infrastructure can be used
Do the developers/vendors recommend any security-related staffing or ancillary equipment for incident prevention or detection?	No data available
Have any subject matter experts (**SMEs)** in voting system/election security recommended a defense in depth security apparatus, specialized staff, or staff training for operating a system such as this?	No data available
Have the developers/vendors or **SMEs** provided any cost or pricing estimates for recommended ancillary security or other operational equipment or staffing?	No data available
Are the system's complexity and operational requirements likely to require an ongoing technical services contract or the outsourcing of operations to a third party vendor?	No data available
Does the system depend of underlying infrastructure (support organizations)?	
a. Public Internet	Yes
b. Wireless communication methods	Can be used
c. Postal services	Yes

d. Various hardware/software	Yes

Helios

0. **Introduction**

Helios was developed by Ben Adida. During his time at Harvard he decided to create an open audit voting system that would reside on the Internet. Building upon the ideas of pioneers such as Josh Benaloh, Ben Adida was able to develop an open source platform for an e2e-v voting system.

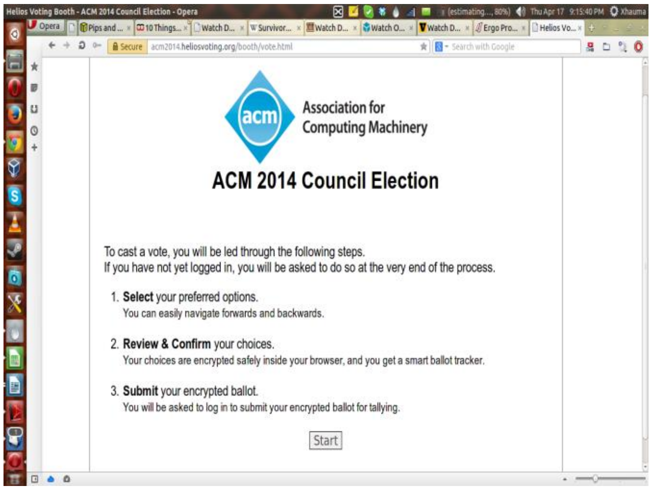
2. **Core Architecture & Operation**

1.1 Basic Architecture & Design:

The Helios system is setup with a website, a python infrastructure, a couple servers, and a built-in encryption system for the votes. The election administrators can from the website, setup an private or public election, invite other users to join the election, run the election, and post the results. The system allows for registration through Google, or facebook and an alternative login system is in the works. All the non-sensitive data is housed on a server owned by Ben Adida and all the private or sensitive data is held on the voters computer.

1.2 Voting Process:

- In a private election, the administrator inputs the email addresses of the voters who will be participating and the system emails the voters their randomly generated login information and the link to the Internet based election.
- Once on the site, the voter follows the on screen prompts and clicks tabs that correspond with their election choices, followed by clicking the next button.
- At the end of the prompts is an option to check if their ballot has been encrypted properly and see if their votes have changed. Following this option allows the voter to verify that their vote was accurate but also destroys the ballot and prompts the voter to vote again. On their second try they can skip the encryption check and click finish. This will send an email to the voter saying that their choices have been casted and that the results will be shown at the end of the election. At any time, a voter can follow their old link and vote, the new vote will replace the old vote.

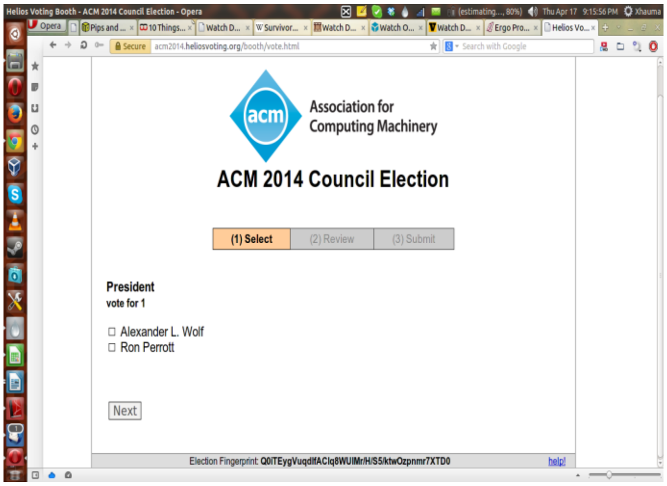

Helios Voting Booth - ACM 2014 Council Election - Opera
(estimating..., 80%) Thu Apr 17 9:15:40 PM Xhauma
Opera
Pips and ...
10 Things...
Watch D...
Survivor...
Watch D...
Watch O...
Watch D...
Ergo Pro...
Helios Vo...
Secure
acm2014.heliosvoting.org/booth/vote.html
Search with Google
Association for Computing Machinery
acm

ACM 2014 Council Election

To cast a vote, you will be led through the following steps.
If you have not yet logged in, you will be asked to do so at the very end of the process.

1. **Select** your preferred options.
   You can easily navigate forwards and backwards.
2. **Review & Confirm** your choices.
   Your choices are encrypted safely inside your browser, and you get a smart ballot tracker.
3. **Submit** your encrypted ballot.
   You will be asked to log in to submit your encrypted ballot for tallying.

Start


Helios Voting Booth - ACM 2014 Council Election - Opera
(estimating..., 80%) Thu Apr 17 9:15:56 PM Xhauma
Opera
Pips and ...
10 Things...
Watch D...
Survivor...
Watch D...
Watch O...
Watch D...
Ergo Pro...
Helios Vo...
Secure
acm2014.heliosvoting.org/booth/vote.html
Search with Google
Association for Computing Machinery
acm

ACM 2014 Council Election

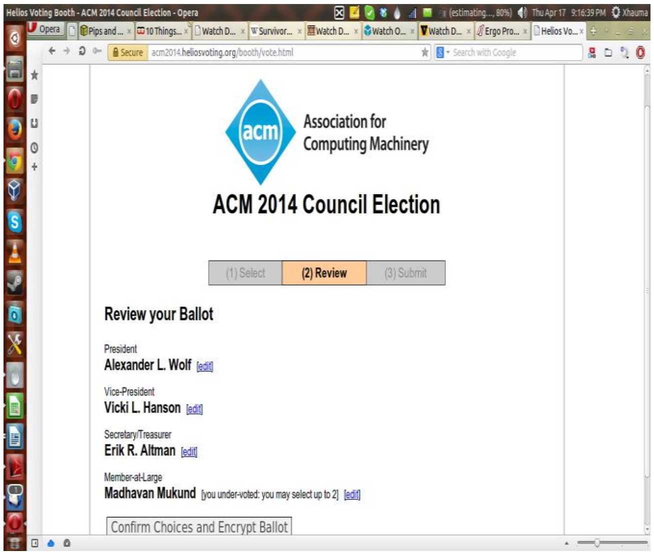
(1) Select | (2) Review | (3) Submit

President
vote for 1

□ Alexander L. Wolf
□ Ron Perrott

Next

Election Fingerprint: Q0iTEygVuqdlfACIq8WUIMr/H/S5/ktwOzpnmr7XTD0 help!


Helios Voting Booth - ACM 2014 Council Election - Opera
(estimating..., 80%) Thu Apr 17 9:16:39 PM Xhauma
Opera
Pips and ...
10 Things...
Watch D...
Survivor...
Watch D...
Watch O...
Watch D...
Ergo Pro...
Helios Vo...
Secure
acm2014.heliosvoting.org/booth/vote.html
Search with Google
Association for Computing Machinery
acm

ACM 2014 Council Election

(1) Select | (2) Review | (3) Submit

Review your Ballot

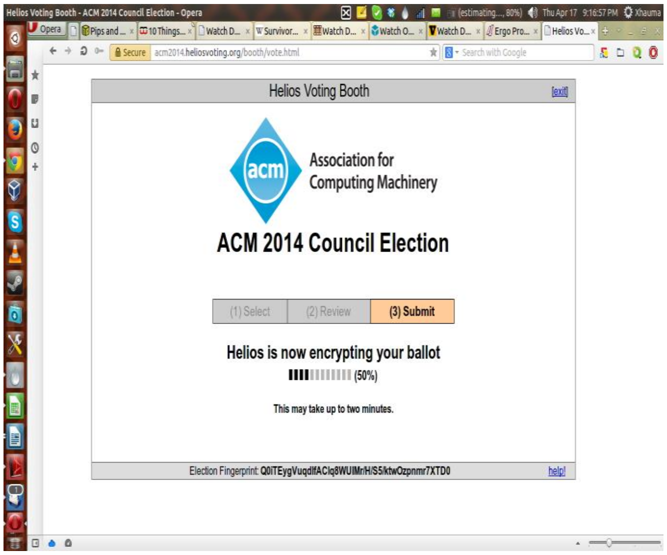
President
Alexander L. Wolf [edit]

Vice-President
Vicki L. Hanson [edit]

Secretary/Treasurer
Erik R. Altman [edit]

Member-at-Large
Madhavan Mukund [you under-voted: you may select up to 2] [edit]

Confirm Choices and Encrypt Ballot


Helios Voting Booth - ACM 2014 Council Election - Opera
(estimating..., 80%) Thu Apr 17 9:16:57 PM Xhauma
Opera
Pips and ...
10 Things...
Watch D...
Survivor...
Watch D...
Watch O...
Watch D...
Ergo Pro...
Helios Vo...
Secure
acm2014.heliosvoting.org/booth/vote.html
Search with Google
Association for Computing Machinery
acm

Helios Voting Booth [exit]

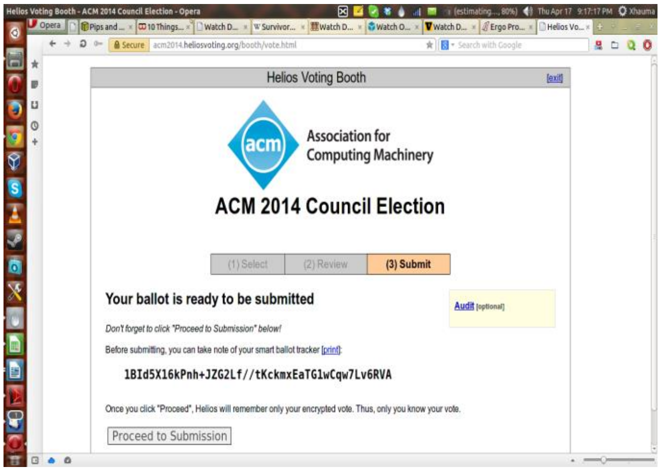
ACM 2014 Council Election

(1) Select | (2) Review | (3) Submit

Helios is now encrypting your ballot
(50%)

This may take up to two minutes.

Election Fingerprint: Q0iTEygVuqdlfACIq8WUIMr/H/S5/ktwOzpnmr7XTD0 help!



Helios Voting Booth - ACM 2014 Council Election - Opera
(estimating..., 80%) Thu Apr 17 9:17:17 PM Xhauma
Opera
Pips and ...
10 Things...
Watch D...
Survivor...
Watch D...
Watch O...
Watch D...
Ergo Pro...
Helios Vo...
Secure
acm2014.heliosvoting.org/booth/vote.html
Search with Google

Helios Voting Booth [exit]

Association for Computing Machinery

ACM 2014 Council Election

(1) Select (2) Review (3) Submit

Your ballot is ready to be submitted

Audit [optional]

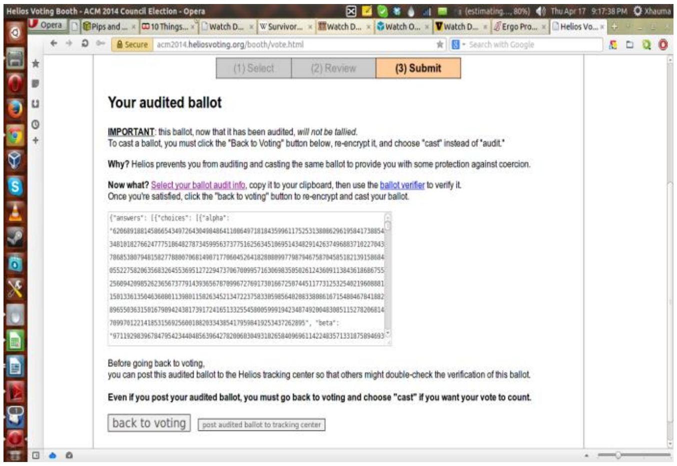
Don't forget to click "Proceed to Submission" below!

Before submitting, you can take note of your smart ballot tracker [print]:

`1BId5X16kPnh+JZG2Lf//tKckmxEaTG1wCqw7Lv6RVA`

Once you click "Proceed", Helios will remember only your encrypted vote. Thus, only you know your vote.

Proceed to Submission



Helios Voting Booth - ACM 2014 Council Election - Opera
(estimating..., 80%) Thu Apr 17 9:17:38 PM Xhauma
Opera
Pips and ...
10 Things...
Watch D...
Survivor...
Watch D...
Watch O...
Watch D...
Ergo Pro...
Helios Vo...
Secure
acm2014.heliosvoting.org/booth/vote.html
Search with Google

(1) Select (2) Review (3) Submit

Your audited ballot

IMPORTANT: this ballot, now that it has been audited, *will not be tallied*.
To cast a ballot, you must click the "Back to Voting" button below, re-encrypt it, and choose "cast" instead of "audit."

Why? Helios prevents you from auditing and casting the same ballot to provide you with some protection against coercion.

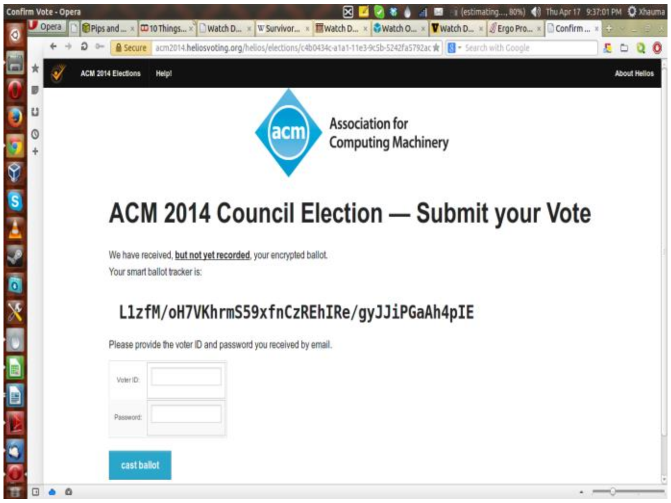
Now what? Select your ballot audit info, copy it to your clipboard, then use the ballot verifier to verify it.
Once you're satisfied, click the "back to voting" button to re-encrypt and cast your ballot.

```
{"answers": [{"choices": [{"alpha":
"6206891881458665434972643049848641100649718184359961175253138886296195841738854
3481018276624777518648278734599563737751625634510695143482914263749688371022704З
7868538079481582778800706814987177066452641828880997798794675870458518213915868
0552275820635683264553695127229473706700995716306983505026124360911384361868675
2560942098526236567377914393656787099672769173016672587445117731253254021960888
1501336135046360801139801158263452134722375833059856402083380861671548046784188
8965503631501679894243817391724165133255458005999194234874920048308511527820681
709970122141853156925600188203343854179598419253437262895", "beta":
"971192983967847954234404856396427820068304931026584096961142248357133187589469
```

Before going back to voting,
you can post this audited ballot to the Helios tracking center so that others might double-check the verification of this ballot.

Even if you post your audited ballot, you must go back to voting and choose "cast" if you want your vote to count.

back to voting post audited ballot to tracking center



ACM 2014 Council Election — Submit your Vote

We have received, **but not yet recorded**, your encrypted ballot.
Your smart ballot tracker is:

L1zfM/oH7VKhrmS59xfnCzREhIRe/gyJJiPGaAh4pIE

Please provide the voter ID and password you received by email.

Voter ID:	
Password:	

2. Security & Trust

2.1 **Security:** When it comes to security Helios does a decent job but is still plague by various security problems. Orion from the University of Washington highlighted a number of weaknesses in his security review blog. "It is possible, just after the voter casts his/her ballot, for a corrupt router to intercept the ballot en route to the Helios server and send the user a fake Helios server success code, causing the "voting booth" to immediately display a false success message and clear the ballot from memory."[5] In this scenario if the user fails to realize that his/her vote has been erased then their vote would end up not counting which would help the adversary manipulate the election. "As it currently exists, if the election administrator allows Helios to administrate the election (as it seems they suggest doing), it is possible for a corrupt Helios server to create new, fake voters and cast ballots on their behalf without easily being discovered."[5] This would allow for a corrupt server to vote for the desired winner and completely debunk the voting process. Also, validation is only carried out by the users, so in the off chance that no one audits the election, the corrupt servers could in fact manipulate with being detected. "As currently implemented, the election administrator (who has the power to add voters and freeze the election) is authenticated through Google Accounts. Any vulnerability in the login (weak password, easily guessed security questions, etc.) could allow an attacker to end the election prematurely or add additional voters (potentially multiple accounts for the same voter)."[5] Due to the reliance on the Google account to actually administer the election, if the administrators account was hijacked then an attacker could do a number of things to hack the system in their favor. Helios is also susceptible to every possible Internet attack in their various forms. Helios does not have advanced or cutting edge means to defend itself against any one Internet attack. This means that any system crashing or infrastructure hacking attacks available can be utilized against Helios. Its only real defense are the general defenses seen in most if not all up to date websites. Helios is patched regularly and is mount on a secure platform in Heroku but outside of this, fulfills the bare requirements of being considered secure.

2.2 **Trust Structure:** "Helios takes an interesting approach: there is only one trustee, the Helios server itself. Privacy is guaranteed only if you trust Helios. Integrity, of course, does not depend on trusting Helios: the election results can be fully audited even if all administrators – in this case the single Helios sever – is corrupt."[1] Helios was constructed in such a way that the only thing a user would have to trust is themselves and the server. Also, because it has an open audit system, they could always double check the results to make sure that the server hasn't been compromised. The assumption that comes with these elements is that they have not been hacked and they are in fact safe. If there is a situation where malware has overtaken either of these items of trust, then the system would be undermined. This isn't a problem unique to Helios but it is a problem none the less.

When it comes to the ballots everything is handled and encrypted by the system itself so at no part of the process does the LEO or Election Official touch or handle the ballots. The only things that they have control over is the keys that decrypt the votes which is only enabled when the election is over. The decrypt keys themselves allow for the votes to be posted, the officials get to see the results the same time the participants see them.

2.3 Dispute Resolution Dispute resolution is handled by the creator and administrator Ben Adida. He has up to this point only had one dispute to resolve and that was handled quickly and everything was straightened out.

2.4 Threat Scenarios - See System Details Chart

3. Auditability "A web-based open-audit voting system. Using a modern web browser, anyone can set up an election, invite voters to cast a secret ballot, compute a tally, and generate a validity proof for the entire process. Helios is deliberately simpler than most complete cryptographic voting protocols in order to focus on the central property of public audit-ability."[1] The entire basis of of Helios is the ability to audit the election after the polls are closed. If the election is public, then anyone with Internet access can check the encrypted votes and verify that the elections was legitimate. The problem with Helios is that though users can audit the system, the process by which one would tends to be complicated to those who are not computer savvy. As mentioned in the usability portion, studies have shown that it is hard for common users to comprehend and properly utilize the auditing tools. Which means that the auditing capability is there but the barriers of use are to high for the users.

References

1. Adida, Ben. "Helios: Web-based Open-Audit Voting." USENIX Security (2008): n. pag. Web. <static.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf>.
2. Adida, Ben. "Helios: A Deeper Look." Telephone interview. Transcript.
3. Karayumak, Fatih, Maina M. Olembo, Michaela Kauer, and Melanie Volkamer. "Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System." CASED:Technische Universit¨at Darmstadt (n.d.): n. pag. Web. <http://www.usenix.org/event/evtwote11/tech/final_files/Karayumak7-27-11.pdf>.
4. Weber, Janna-Lynn, and Urs Hengartner. "Usability Study of the Open Audit Voting System Helios." JannaWeber.com. Janna-Lynn Weber, Sept. 2009. Web. <http://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf>.
5. University of Washington, Orion. "Security Review: Helios Online Voting." UW Computer Security Research and Course Blog. University of Washington, 13 Mar. 2009. Web. <https://cubist.cs.washington.edu/Security/2009/03/13/security-review-helios-online-voting/>.
6. SecVote, Dagsthul. "Usable Verifiable Remote Electronic Voting Case Study HELIOS." SecVote. SecVote, 18 July 2012. Web. <http://secvote2010.uni.lu/slides/mvolkamer-usability.pdf>.

System Details Template -> Helios

I. CORE ARCHITECTURE & OPERATION FEATURES

Issue	**Summary Answers**
Features of the system; paper, pure electronic, etc?	This system is an electronic system that completely resides on the Internet.
Programming Language(s)	The system is written in Python and is integrated on top of the django web framework.
Encryption Method(s)	AES is applied to the ballots after the votes have been picked.
Which of the following stages of the voting process are encrypted? 1) Blank ballots at time of distribution to voter, 2) Voted ballot after ballot selections (votes) are marked, as part of casting, 3) Vote recording at the LEO, 4) Tabulation processes.	The voted ballot after ballot selections are marked. It is still encrypted during the casting, the vote recording by the LEO and the tabulation process.
Does the VS supply adequate and clear documentation to LEOs to facilitate efficient, accurate set up of an election & operation?	At the time of the writing of the report there doesn't seem to be any Helios issued facilitation documentation.
Does the VS supply dedicated voter education materials (or online tutorials) to introduce the system's operation to voters?	There is a video tutorial for using the system at: https://vimeo.com/61591845.
	To date, the largest amount of voters in the system has been 30,000+.

How scalable is the system? What voting population and expected ballot cast numbers can it accommodate?	

II. SECURITY DESIGN & SECURITY TESTING

Issue:	Summary Answers
Describe the security architecture & design features.	The system is developed with basic security architecture & design features. They do not exceed outside of that.
Do developers explicitly claim the system programming complied with security best practices? E.g., OWASP Top Ten or other guides? If so, which best practice guides explicitly mentioned in documentation?	The developers do not explicitly claim that the system programming is complied with security best practices.
What error/anomaly detection and error correction capabilities are built-in?	N/A
How does the voting system provide resistance towards malware at voter/client side?	There is no additional resistance towards malware on the voter/client side.
How does the voting system provide resistance towards malware at election official/server side?	There is no additional resistance towards malware on the official/server side.
How does the voting system provide resistance to client/voter side denial of service (DOS) attacks?	The system doesn't provide resistance to client/voter side denial of service attacks.
How does the voting system provide resistance to election official/server side DOS attacks?	The system doesn't provide resistance to official/server side denial of service attacks.
What methods of resilience against coercion to voters and local election officials are available with this system?	The system was not created with any resilience against coercion.
Has there been a network and/or application security assessment by security experts for this system?	There has been one assessment by a researcher from the University of Washington.

Were the results of the security assessment publically published?	They have been released on the school technology blog: https://cubist.cs.washington.edu/Security/2009/03/13/security-review-helios-online-voting/
Were details for a security patching process provided for this system?	The system is patched directly from the creator and is published immediately.
Does the system provide data redundancy in the case of a disaster?	N/A
Do the developers/vendor offer recommendations to LEOs re key management? ***If yes,*** do they mention operational processes, privilege/separation of duty, or special equipment/software for key management?	N/A
If the LEOs private keys were to be compromised by a hacker or insider in some manner, describe the damage to the integrity/accuracy of the vote totals/results that could be achieved. If unauthorized key access could lead to tampering with vote totals, would that tampering be detectable? If so, what kind of analysis would be required to identify/detect that tampering?	In the case of such an emergency, all that could be done is the prevention of the election ending. The keys have no way of tampering with the vote toals directly. The keys in Helios are used for concluding the election and releasing the results. It has no direct use with the vote.

III. TRUST STRUCTURE

When this system is deployed, who (and what equipment or processes) must the voter, the general public and election officials, trust to be working correctly – without any additional or independent verification other than what this voting system provides-- that all votes have been recorded, transmitted, tallied and reported accurately?

Issue	**Summary Answers**
Whom (or what equipment & processes) must the voter trust that: the correct blank ballot is delivered with all races and issues present?	THE VOTER HAS TO TRUST THEIR OWN COMPUTER, AND THE HELIOS SERVERS.
their choices (candidates and/or issues) are recorded correctly before the marked ballot leaves their device?	THE VOTER HAS TO TRUST THEIR OWN COMPUTER, AND THE HELIOS SERVERS.
their ballot as been received by local election office?	THE VOTER HAS TO TRUST THEIR OWN COMPUTER, AND THE HELIOS SERVERS.
that their ballot has been a part of the tabulation?	THE HELIOS SERVERS.
that their ballot choices have been tallied correctly in the total cast ballots results?	THE HELIOS SERVERS.
Whom must the local election official trust that the ballot presents the correct ballot choices for a given voter?	THE LOCAL ELECTION OFFICIAL HAS TO TRUST THEIR OWN COMPUTER, AND THE HELIOS SERVERS.
Whom must voter & general public trust that the votes have been tallied & reported to the public correctly?	THE HELIOS SERVERS.

IV. AUDITABILITY

Issue	Summary Answers
1. What types of protections does the Voting System "**VS**" (or via the operational/managerial election processes it recommends) provide for assuring that the voter's ballot choices are not modified in an undetectable manner? ***Specifically***	There is a built-in encryption verification system that can be accessed before casting the vote.
a. Does the system produce a voter-verifiable, durable, tamper-evident artifact (abbreviated "**V V-D-TEA**")?[6] ***If yes,*** describe the type of artifact it produces (e.g. physical or digital)?	There is not artifact to prove that your vote hasn't be tampered with.
b. Can any additions, deletions, or substitutions to the voter's ballot selections (votes) be detected, using the **V V-D-TEA** records?	There is an email that lets the voter know they have recently voted. If the voter didn't recently vote, then they would've detected a fraud.
c. Can the results of the election contests (races and issues) be reconstructed (recounted) independently of using the voting system's software, simply by using the **V V-D-TEA** records?[7]	Yes, there is a built-in encryption verification system that can be accessed by all participants.
d. Does the system require additional audit checks, for instance by using digital signatures and hashes? ***If yes***, explain what additional integrity checks (at what junctures and for what purposes) have been designed into the system.	There is a hash element and it comes into play at the end of the election when checking ones vote.
2. Does the voting system support the auditing of:	
a. # of blank ballots sent to voters	No
b. # of voted ballots received from voters	No
c. Verifiability of votes as recorded ??	Yes
d. Verifiability of cast as recorded	Yes

[6] Noted voting system auditing expert Dr. Phillip Stark recommended this set of attributes that we have abbreviated "V V-D-TEA."

[7] This question asks for whether the system can be described as producing a voting record and potential for election results that are "software independent." *See* Rivest & Stark, and Stark & Wagner (cites)

e. Verifiability of tallied as cast	Yes
3. Does the auditability design of the voting system require via hard-coded [non-discretionary, within range of reasonability] logs of operators' interaction with:	
a. blank ballots generator/database	N/a
b. voted ballots collection system/database	N/a
c. cast ballots storing system/database	N/a
d. cast ballots tallies	N/a
e. cast ballots reports	N/a
f. system failures, malfunctions and other threat or attack on the operation of the voting system, as well as other infrastructure components	N/a
4. Are these audit logs protected from administrative or operator modifications (insider threat)? If yes, explain how.	Yes, the operator has no way of altering the audits due to the helios infrastructure.
5. Are these audit logs protected against operations (e.g., system crashes) or attacks which could lead to data corruption or loss? If yes, explain how.	No
6. Does the audit system maintain voter anonymity at all times? If yes, explain how	Yes it does. By maintaining aliases for all voters on top of keeping the actual votes encrypted, the anonymity is maintained at all times.

V. VOTER ANONYMITY

Issues:	Summary Answer
1. Does the voting system maintain voter’s anonymity while • Voter is accessing the system to obtain or mark a ballot?	No
• Voter is marking and casting his/her vote?	NO
• the vote is being recorded at the LEO?	Yes
• the vote is being tallied?	Yes
2. Does the voting system maintain anonymity after the final results are posted?	Yes
3. Can voters/users post feedback or make complaints anonymously?	No
4. Does the system monitor the voter/user while the system is in use?	No
5. Could an adversary track/trace a user and connect the user to a particular cast ballot after compromising the system?	No
6. Does the system use a third party application that could thwart a user's privacy?	The system is heavily dependent on gmail for having the voter get into the voting system and to alert the voter of their completed ballot. If the gmail account is compromised, then it would thwart a user's privacy.

VI. TESTING, CERTIFICATION & DEPLOYMENTS

Issues:	**Summary Answers**
Testing *(exclusive of testing discussed under* **Security** *&* **Usability***)*	
1. Has the system received reliability testing or any other testing specified by the Voluntary Voting System Guidelines (VVSG)?	no
2. If yes, what VVSG-specified testing and with what results?	N/a
3. Has the system been submitted for certification under the EAC voting system process? If so, provide details of when and with what results.	no
4. Has the system received open-ended vulnerability testing, as recommended by the EAC's Technical Guidelines Development Committee?	no
5. If yes, detail by whom/ when/ where?	N/a
6. Has the system undergone any other independent testing, not by the internal developers but by a qualified independent organization or set of individuals? If so, describe with dates and published reports.	no
7. Have the developers announced any planned independent testing? If so, when?	no

Certifications	
8. Has the system undergone any certification testing? If so, in what State or jurisdiction, and with what results?	N/a
9. Has the system been certified for use by some States or jurisdictions? If so where?	N/a
Current or planned deployments?	
Public Government elections? If so, where and dates?	no
Private/ nonprofit/ labor unions, etc. If so, where/when?	Yes, it will be deployed in Europe for a big election but no further data is given.

VII. Usability/ Accessibility

Issues:	**Summary Answers**
Usability: 1. Has a usability study been conducted by qualified usability assessors and published by public or scholarly access?	yes
2. If yes, did the study report deficiencies in the system with regard to usability?	yes
• Comprehension & success in marking of ballot?	yes
• Comprehension & success in casting of ballot?	yes
• Comprehension & success in verifying of ballot?	yes
3. Did the study report usability deficiencies in the system with regard to election official set up of the election?	no
4. Discuss the quality and completeness of the documentation for LEOs to set up the system, create of ballots and tabulation, voter education, and other aspects.	N/a
Accessibility: 4. Is the system designed for persons with physical impairments that may affect voting? Specifically	
a. Blind	no
b. Deaf	yes
c. Multiple impairments	N/a
	N/a

5. Has an accessibility study been conducted by qualified accessibility assessors, published by public or scholarly access? ***If so,*** cite.	

VIII. Infrastructure:

Staffing, Training & Equipment Needed to Conduct Elections Successfully & Securely

Issue	Summary Answers
Equipment needed by Voter to receive, mark & cast ballot	A computer and an email address
Equipment needed by LEO to develop ballots, send to voters, receive marked ballots, & tabulate plus report?	A computer and possibly a server.
Do the developers/vendors recommend any security-related staffing or ancillary equipment for incident prevention or detection?	no
Have any subject matter experts (**SMEs)** in voting system/election security recommended a defense in depth security apparatus, specialized staff, or staff training for operating a system such as this?	no
Have the developers/vendors or **SMEs** provided any cost or pricing estimates for recommended ancillary security or other operational equipment or staffing?	Yes, the developer provides a cost for other operational equipment
Are the system's complexity and operational requirements likely to require an ongoing technical services contract or the outsourcing of operations to a third party vendor?	N/a
Does the system depend of underlying infrastructure (support organizations)?	
7. Public Internet	yes

8. Wireless communication methods	yes
9. Postal services	no
10. Various hardware/software	no

RIES

0. Introduction:

RIES, the Rijinland Internet Election System was developed by the Hoogheemraadschap van Riginland, one of Neitherland's regional water management authorities. RIES is patented by Piet Maclaine Point and Riginland Water Board [RN1]. The basic design idea is derived from the master thesis [RN6] of Maclaine Pont's student, Herman Robers. It was first introduced as a solution to the low turnout rate of Water Board Elections in 2004. About 72,000 online votes were cast, out of 2.2 million eligible voters. In November 2006, RIES was used by Dutch voters reside outside of Netherland, to participate in the Lower House Parliamentary Elections. Around 20,000 voters voted via Internet, which accounts for 91% of the total eligible voters [RN4]. The source code of RIES was published on June 2008 [RN2]. One of the main distinguishing features of RIES is that it enables voters and to verify after the election is closed that their own votes have been counted correctly, and that the result of the tally corresponds to the cast votes.

1. Core Architecture & Operation

The main voting system uses Javascript. Cryptographic mechanisms such as DES, 3DES, DESmac, MDC-2, RSA and SHA-1 are deployed through the voting cycle.

In general, the voting process consists of the following steps:

- Before the voting, the administrative agency will use crypto-hardware to generate a personal key for each voter. These keys are printed on ballots and distributed by mail. Furthermore, it will generate ballot collections [RN1] for each voter, combine all the ballot collections to a pre-election reference table and then publish the table on the Internet.
- During the voting, voter will use the RIES web interface to enter its personal key from the ballots, and then select the candidate. When successful, the browser will return a technical vote on screen which serves as a receipt. Furthermore, voter should destroy his ballot with secret key and store the technical vote for future verification. All the technical votes are stored on the network server SURFnet.
- After the election is closed, SURFnet will hand over all technical votes to the administrative agency. The administrative agency computes a hash of every technical vote, validate it using the pre-election reference table and then compute the voting outcome. Finally, the voting office will publish the total outcome.

2. Security & Trust

2.1 Security

As further illustrated in point 5, RIES were subject to several security related testing before deployment and evaluation results are positive according to the official website. Without access to those testing results, we are not aware that to what extent RIES is resistant to DDoS and

Malware attacks at Server side. But since RIES assumes that voter's PC is secure, we can conclude that it is not resistant to Malware or 'Man-in-the-middle-attack' at Client side.

2.2 Trust Structure

For voters vote via Internet, although verifiability is achieved through the voting cycle, they still need to trust the administrative party/vendor to handle their personal secret key securely.

For voters vote via postal ballots, they need to trust the Postal Votes Processing Bureau to convert their mail votes to technical votes correctly because they can't validate what has been done to their votes.

2.3 Dispute Resolution

When disputes arise, an umpire can check and recalculate various steps in the whole process and pass his own judgment, but this only works for a limited type of disputes. [RN3]

2.4 Documented Security Issues and Hacks

Before the 2008 Word Board elections, the ministry hired Fox-IT to perform the formal approval of RIES-2008, the company had found very serious problems with the underlying cryptography.[8] [RN2, p3]

In addition, a study of RIES' published source code in 2008 [RN2] reveals serious security holes that make the system vulnerable to Cross-Site Scripting, SQL injection and predictable token generation.

3. Vote Privacy

Voter privacy has been a significant area of concern for RIES voting system. First, vote secrecy is highly depending on the way the personal keys are handled. Although the administrative party/vendor that generate the personal keys are required to destroy these keys post-election, threats like insider activities or malware attacks on the server make the vote secrecy in jeopardy . In addition, vote server can link the originating IP address to the vote that is cast. The lack of anonymous channel creates another risk for voter privacy. [RN3]

4. Auditability.

[8] The report is in Dutch. Gedrojc, B., Hueck, M., Hoogstraten, H., Koek, M., Resink, S.: Rapportage
Fox-IT - Advisering toelaatbaarheid internetstemvoorziening waterschappen (2008), http://www.verkeerenwaterstaat.nl/Images/20081302%20Bijlage%201%20rapport_tcm195-228336.pdf

Each individual voter can verify, with his stored technical vote, whether his actual vote has been correctly casted. This is achieved by comparing the hash value on his technical vote with the hash value in the pre-election reference table.

The tally verification can be done by everyone interested. Theoretically, interested party can download all technical votes from the network server provider SURFnet, compute the hash value for each vote, and then compare the results with the pot-election reference table. However, this does not enable anyone to verify that the votes are truly as intended.

5. Testing and Deployments: Performance/Functionality and Security

According to the official website www.openries.nl, a number of independent organizations have evaluated the RIES voting system before its deployment:

> "Various prominent institutions have tested and positively evaluated RIES: TNO Human Factos from Soesterberg tested usability of the voting interface; A team of specialists from Peter Landrocks Cryptomathic(in Aarhus, Denmark) tested the cryptographic principles; Madison Gurka from Eindhoven tested the server and network setup and security; A team under supervision of Bart Jacobs(Radboud University Nijmegen) did external penetration tests." (Originally written in Dutch, translation cited from [RN2])

It appears that scientists as well as independent third parties have looked into various aspects of the design and security of RIES, both before and after the deployment. However, most of the testing reports and scientific works are published within Netherland therefore are written in Dutch. This certainly creates an obstacle for the project team to access and interpret those documents.

6. Usability & Accessibility Assessments (including testing for these attributes)

As mentioned in point 5, there were usability and accessibility tests conducted on RIES voting system, but the project team could not find one addressed to the international audience. Based on the available resources, we know that RIES can accommodate both Internet voting and the traditional postal ballots voting. It is accessible to the disabled community in a sense that people can vote at home via Internet using their own accessibility technologies.

7. Infrastructure Requirements

Unknown

System Details Template -> RIES

I. CORE ARCHITECTURE & OPERATION FEATURES

Issue	Summary Answers
Features of the system; paper, pure electronic, etc?	RIES features both paper based postal voting and remote electronic voting
Programming Language(s)	Java
Encryption Method(s)	DES, 3DES, DESmac, MDC-2, RSA, SHA-1, SSL[RN3, p8-9]
Which of the following stages of the voting process are encrypted? 1) Blank ballots at time of distribution to voter, 2) Voted ballot after ballot selections (votes) are marked, as part of casting, 3) Vote recording at the LEO, 4) Tabulation processes.	1, 2 and 3
Does the VS supply adequate and clear documentation to LEOs to facilitate efficient, accurate set up of an election & operation?	Yes. The structure and organizations of RIES-2008 are reasonably clear. Extensive documents are provided by the designers and organizers. [RN3, p46]
Does the VS supply dedicated voter education materials (or online tutorials) to introduce the system's operation to voters?	Insufficient information

How scalable is the system? What voting population and expected ballot cast numbers can it accommodate?	Insufficient information

II. SECURITY DESIGN & SECURITY TESTING

Issue:	Summary Answers
Describe the security architecture & design features.	• Before the election starts, a Reference is published, will allow for several checks on the entire election system • None of the voter secrets leave the voter's PC browser • allows for the acceptance and processing of multiple voting entries from the same voter in the same election • RIES allows for the issuing of a replacement election package • allows for the validation that an election package can only be used to cast a valid vote by the voter • results are end-to-end auditable by any interested party
Do developers explicitly claim the system programming complied with security best practices? E.g., OWASP Top Ten or other guides? If so, which best practice guides explicitly mentioned in documentation?	Insufficient information
What error/anomaly detection and error correction capabilities are built-in?	The system has a help desk built-in to deal with replacing ballot forms. System error and communication error is logged
How does the voting system provide resistance towards malware at voter/client side?	It is not resistant. RIES assumes the voter pc is secure.[RN3, p51]
How does the voting system provide resistance towards malware at election official/server side?	Insufficient information
How does the voting system provide resistance to client/voter side denial of service (DOS) attacks?	Not resistant.
	performed by SURFnet

How does the voting system provide resistance to election official/server side DOS attacks?	(www.surfnet.nl) through two server-complexes in different protected locations on distinctly different network paths, and internal defenses against spoofing and the detection of DDOS attack [RN7, p3]
What methods of resilience against coercion to voters and local election officials are available with this system?	It is not available. If an attack gains access to received votes or the voting servers before the tally phase starts, it has the capability to forge votes.[RN3, p51]
Has there been a network and/or application security assessment by security experts for this system?	Yes. A team of specialists from Peter Landrocks Cryptomathic(in Aarhus, Denmark) tested the cryptographic principles; Madison Gurka from Eindhoven tested the server and network setup and security; A team under supervision of Bart Jacobs(Radboud University Nijmegen) did external penetration tests.
Were the results of the security assessment publically published?	Some of them are said to be published. But an international version is not available.
Were details for a security patching process provided for this system?	Insufficient information
Does the system provide data redundancy in the case of a disaster?	Yes. • There are four redundant voting windows server and three redundant isolated servers for sensitive operation, all online. • For workflow managing, there are two redundant machines, but only one of them is online. The second one is configured as hot-standby and can be made active when needed. Due to the sensitive nature of the data on the servers no backups are made. In case of the loss of a server it will be rebuilt from scratch using a provisioning server. Data loss is prevented by several mechanisms, specifically using redundant hardware and synchronization between locations.[RN3 p47]

Do the developers/vendor offer recommendations to LEOs re key management? ***If yes,*** do they mention operational processes, privilege/separation of duty, or special equipment/software for key management?	Insufficient information
If the LEOs private keys were to be compromised by a hacker or insider in some manner, describe the damage to the integrity/accuracy of the vote totals/results that could be achieved. If unauthorized key access could lead to tampering with vote totals, would that tampering be detectable? If so, what kind of analysis would be required to identify/detect that tampering?	LEOs doesn't have private key. However, if an attack gains access to received votes or the voting servers with the insider's help, before the tally phase starts, it can forge votes therefore damage the integrity and accuracy of the tally results. In RIES, the mitigation process are organizational.[RN3 p48]

III. TRUST STRUCTURE

When this system is deployed, who (and what equipment or processes) must the voter, the general public and election officials, trust to be working correctly – without any additional or independent verification other than what this voting system provides-- that all votes have been recorded, transmitted, tallied and reported accurately?

Issue	Summary Answers
Whom (or what equipment & processes) must the voter trust that: • the correct blank ballot is delivered with all races and issues present?	• RIPOCS: This is the isolated server for sensitive operations like key generation • PSB: Printing service bureau
• their choices (candidates and/or issues) are recorded correctly before the marked ballot leaves their device?	• Voter • Voter PC
• their ballot as been received by local election office?	• PORTAL: the workflow manager. Its tasks include integration of all received votes, prepare publications and offer them LEOs. • SURFnet: support the technical infrastructure of both the PORTAL as well as the Voting Windows server (application that receive internet votes)
• that their ballot has been a part of the tabulation?	• RIPOCS: for the integrity of the VS cryptographic design • PORTAL
• that their ballot choices have been tallied correctly in the total cast ballots results?	• RIPOCS: for the integrity of the VS cryptographic design • PORTAL • UMPIRE: to verify this on behalf voters (typically those who lose the technical vote)
Whom must the local election official trust • that the ballot presents the correct ballot choices for a given voter?	• RIPOCS: for the integrity of the VS cryptographic design • PORTAL
Whom must voter & general public trust that the votes have been tallied & reported to the public correctly?	• RIPOCS: for the integrity of the VS cryptographic design • PORTAL

IV. AUDITABILITY

Issue	Summary Answers
1. What types of protections does the Voting System “**VS**” (or via the operational/managerial election processes it recommends) provide for assuring that the voter's ballot choices are not modified in an undetectable manner? ***Specifically***	
a. Does the system produce a voter-verifiable, durable, tamper-evident artifact (abbreviated "**V V-D-TEA**")?[9] ***If yes,*** describe the type of artifact it produces (e.g. physical or digital)?	Yes. A digital artifact called technical vote.
b. Can any additions, deletions, or substitutions to the voter's ballot selections (votes) be detected, using the **V V-D-TEA** records?	If sufficiently many voters use this right, fraud should become detectable. But the assumption here should be the reference table hash function is not compromised.
c. Can the results of the election contests (races and issues) be reconstructed (recounted) independently of using the voting system's software, simply by using the **V V-D-TEA** records?[10]	Yes
d. Does the system require additional audit checks, for instance by using digital signatures and hashes? ***If yes***, explain what additional integrity checks (at what junctures and for what purposes) have been designed into the system.	Yes. The one-time digital signature schemes are used for the authentication of the voted ballots. Hash MDC-2 is used be computing the technical vote and therefore used in the counting process
2. Does the voting system support the auditing of:	

[9] Noted voting system auditing expert Dr. Phillip Stark recommended this set of attributes that we have abbreviated “V V-D-TEA."

[10] This question asks for whether the system can be described as producing a voting record and potential for election results that are “software independent.” *See* Rivest & Stark, and Stark & Wagner (cites)

a. # of blank ballots sent to voters	Yes
b. # of voted ballots received from voters	Yes
c. Verifiability of votes as recorded	Insufficient information
d. Verifiability of cast as recorded	Insufficient information
e. Verifiability of tallied as cast	Yes
3. Does the auditability design of the voting system require via hard-coded [nondiscretionary, within range of reasonability] logs of operators' interaction with:	
a. blank ballots generator/database	A paper log of each replacement step is kept in the Helpdesk, which is signed by the individual Helpdesk member that handles it.[RN3]
b. voted ballots collection system/database	If a vote is declared invalid, a log entry is created indicating why it was invalid and hence not counted.[RN1 p7]
c. cast ballots storing system/database	Insufficient information
d. cast ballots tallies	Insufficient information
e. cast ballots reports	Insufficient information
f. system failures, malfunctions and other threat or attack on the operation of the voting system, as well as other infrastructure components	System errors as well as other reductions in the operability of the server side are logged [RN5 p55]
4. Are these audit logs protected from administrative or operator modifications (insider threat)? If yes, explain how.	Insufficient information
5. Are these audit logs protected against operations (e.g., system crashes) or attacks which could lead to data corruption or loss? If yes, explain how.	Insufficient information
	Insufficient information

6. Does the audit system maintain voter anonymity at all times? If yes, explain how	

V. VOTER ANONYMITY

Issues:	**Summary Answer**
1. Does the voting system maintain voter's anonymity while • Voter is accessing the system to obtain or mark a ballot?	Yes. Under the assumption that voter private key is properly handled.
• Voter is marking and casting his/her vote?	No, voting server can link the IP address with the vote casted [RN3 p49]
• the vote is being recorded at the LEO?	No. vote is stored in clear text
• the vote is being tallied?	No. vote is stored in clear text
2. Does the voting system maintain anonymity after the final results are posted?	Insufficient information
3. Can voters/users post feedback or make complaints anonymously?	No. Must reveal identity information to UMPIRE
4. Does the system monitor the voter/user while the system is in use?	Insufficient information
5. Could an adversary track/trace a user and connect the user to a particular cast ballot after compromising the system?	Yes.
6. Does the system use a third party application that could thwart a user's privacy?	No

VI. TESTING, CERTIFICATION & DEPLOYMENTS

Issues:	**Summary Answers**
Testing *(exclusive of testing discussed under* **Security** *&* **Usability***)*	
1. Has the system received reliability testing or any other testing specified by the Voluntary Voting System Guidelines (VVSG)?	Insufficient information
2. If yes, what VVSG-specified testing and with what results?	
3. Has the system been submitted for certification under the EAC voting system process? If so, provide details of when and with what results.	Insufficient information
4. Has the system received open-ended vulnerability testing, as recommended by the EAC's Technical Guidelines Development Committee?	Insufficient information
5. If yes, detail by whom/ when/ where?	
6. Has the system undergone any other independent testing, not by the internal developers but by a qualified independent organization or set of individuals? If so, describe with dates and published reports.	Yes. Due to the language barrier, here are the information we could found: "Various prominent institutions have tested and positively evaluated RIES: TNO Human Factos from Soesterberg tested usability of the voting interface; A team of specialists from Peter Landrocks Cryptomathic(in Aarhus, Denmark) tested the cryptographic principles; Madison Gurka from Eindhoven tested the server and

	network setup and security; A team under supervision of Bart Jacobs(Radboud University Nijmegen) did external penetration tests. (Originally written in Dutch, translation cited from [RN2 p160])
7. Have the developers announced any planned independent testing? If so, when?	No
Certifications	
8. Has the system undergone any certification testing? If so, in what State or jurisdiction, and with what results?	No
9. Has the system been certified for use by some States or jurisdictions? If so where?	No
Current or planned deployments?	
Public Government elections? If so, where and dates?	No
Private/ nonprofit/ labor unions, etc. If so, where/when?	No

VII. Usability/ Accessibility

Issues:	**Summary Answers**
Usability: 1. Has a usability study been conducted by qualified usability assessors and published by public or scholarly access?	Yes. TNO Human Factos from Soesterberg tested usability of the voting interface. However, an international version is not available. [RN2 p160]
2. If yes, did the study report deficiencies in the system with regard to usability?	
d. Comprehension & success in marking of ballot?	
e. Comprehension & success in casting of ballot?	
f. Comprehension & success in verifying of ballot?	
3. Did the study report usability deficiencies in the system with regard to election official set up of the election?	
4. Discuss the quality and completeness of the documentation for LEOs to set up the system, create of ballots and tabulation, voter education, and other aspects.	
Accessibility: 4. Is the system designed for persons with physical impairments that may affect voting? Specifically	
a. Blind	
b. Deaf	
c. Multiple impairments	

5. Has an accessibility study been conducted by qualified accessibility assessors, published by public or scholarly access? ***If so,*** cite.	No.

VIII. Infrastructure:

Staffing, Training & Equipment Needed to Conduct Elections Successfully & Securely

Issue	Summary Answers
Equipment needed by Voter to receive, mark & cast ballot	Voter PC and Internet Connection, detailed features of client's browser can be found in [RN3 p38]
Equipment needed by LEO to develop ballots, send to voters, receive marked ballots, & tabulate plus report?	• Portal • Private Network • Cryptographic Hardware • Printing Service Bureau • Postal Votes Processing Bureau • Backup/redundancy
Do the developers/vendors recommend any security-related staffing or ancillary equipment for incident prevention or detection?	Insufficient information
Have any subject matter experts (**SMEs)** in voting system/election security recommended a defense in depth security apparatus, specialized staff, or staff training for operating a system such as this?	Insufficient information
Have the developers/vendors or **SMEs** provided any cost or pricing estimates for recommended ancillary security or other operational equipment or staffing?	Insufficient information
Are the system's complexity and operational requirements likely to require an ongoing technical services contract or the outsourcing of operations to a third party vendor?	No.
Does the system depend of underlying infrastructure (support organizations)?	
e. Public Internet	yes
f. Wireless communication methods	yes
g. Postal services	yes
h. Various hardware/software	yes

Group II Systems

Norway

0. Introduction:

As one of most successful government attempting with Internet Voting, Norway started its first pilot internet election during September 2011 Local and Regional Elections in ten municipalities, with the goal to boost the declining electoral turn-outs, and to streamline electoral administration to ensure more efficient and reliable registration and counting of votes. It continued piloting Internet voting in the 2013 Parliament Election in 12 municipalities, with over 250,000 eligible voters. The Electronic Election Administration System (EVA) is designed, developed, maintained, and managed by the Ministry of Local Government and Regional Development, EDB Ergo Group, and Scytl. The Ministry of Local Government and Regional Development (MLGRD) is responsible for the overall organization of elections and for proposing electoral reforms.

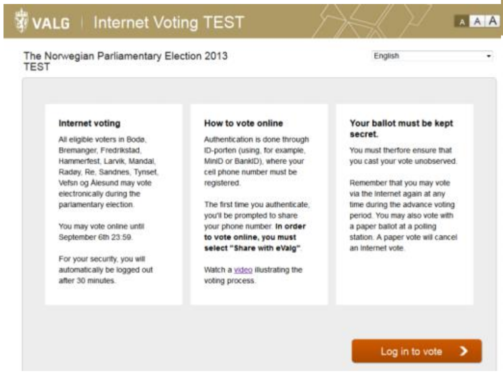
1. Core Architecture & Operation

1.1 Basic Architecture & Design;

The 2013 Parliament Election uses complex ballot, which is a preferential list system where voters can choose one or more candidates across multiple lists. Voters have 25 days of advance voting period both via Internet and paper. Voters can cast multiple electronic votes, and cancel them by voting on paper, both in advance and on Election Day. The election administration system (Elektronisk Valgadministrasjonssystem - EVA) deployed has four central components: encompassing an electronic voter list, scanning of ballot papers, electronic vote counting and result reporting. The system is written primarily in Java, also in C# and Perl. The cryptographic protocol is designed by Scytl. (More details in Section 2)

1.2 Voting Process:

- A polling card was mailed to voters with instruction on how to vote and a set of securely printed, unique return codes for each political party. The return codes were four digit numbers and were unique for each voter.



The Norwegian Parliamentary Election 2013
TEST

Internet voting

All eligible voters in Bodø, Bremanger, Fredrikstad, Hammerfest, Larvik, Mandal, Radøy, Re, Sandnes, Tynset, Vefsn og Ålesund may vote electronically during the parliamentary election.

You may vote online until September 6th 23:59.

For your security, you will automatically be logged out after 30 minutes.

How to vote online

Authentication is done through ID-porten (using, for example, MinID or BankID), where your cell phone number must be registered.

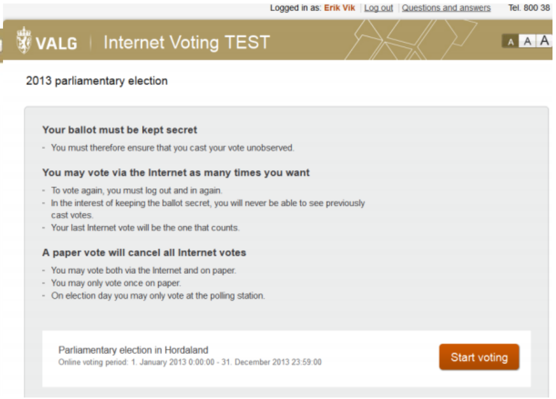
The first time you authenticate, you'll be prompted to share your phone number. **In order to vote online, you must select "Share with eValg".**

Watch a video illustrating the voting process.

Your ballot must be kept secret.

You must therfore ensure that you cast your vote unobserved.

Remember that you may vote via the Internet again at any time during the advance voting period. You may also vote with a paper ballot at a polling station. A paper vote will cancel an Internet vote.



2013 parliamentary election

Your ballot must be kept secret

- You must therefore ensure that you cast your vote unobserved.

You may vote via the Internet as many times you want

- To vote again, you must log out and in again.
- In the interest of keeping the ballot secret, you will never be able to see previously cast votes.
- Your last Internet vote will be the one that counts.

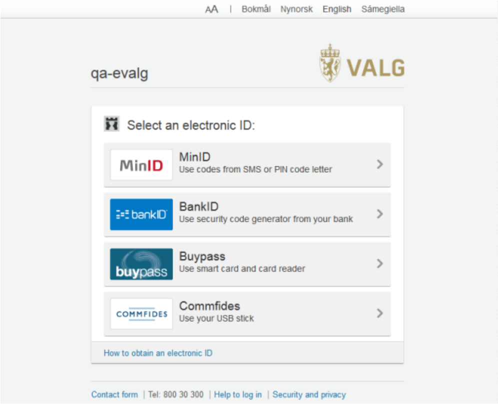
A paper vote will cancel all Internet votes

- You may vote both via the Internet and on paper.
- You may only vote once on paper.
- On election day you may only vote at the polling station.

Parliamentary election in Hordaland
Online voting period: 1. January 2013 0:00:00 - 31. December 2013 23:59:00

Figure 1: Main Interface of the Norway Internet Voting system [11] [NC1, p26-27]

- Voters must identify themselves with one type of electronic ID before voting. After the authentication, the system will guide the user through a simple and intuitive process where he/she can choose which party to vote for, indicate the preference by assigning order to each candidate or deleting candidate from the ballot. (Seen in Figure 2)

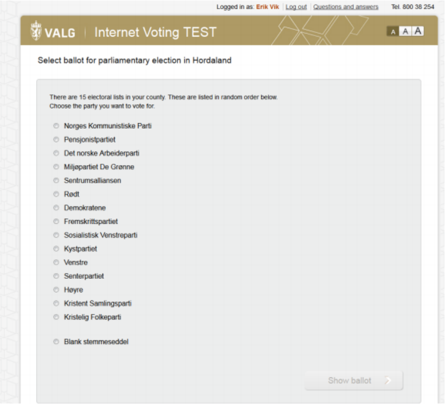


Select an electronic ID:

- MinID – Use codes from SMS or PIN code letter
- BankID – Use security code generator from your bank
- Buypass – Use smart card and card reader
- Commfides – Use your USB stick

How to obtain an electronic ID

Contact form | Tel: 800 30 300 | Help to log in | Security and privacy


Logged in as: Erik Vik | Log out | Questions and answers Tel. 800 38 254
VALG | Internet Voting TEST
A A A

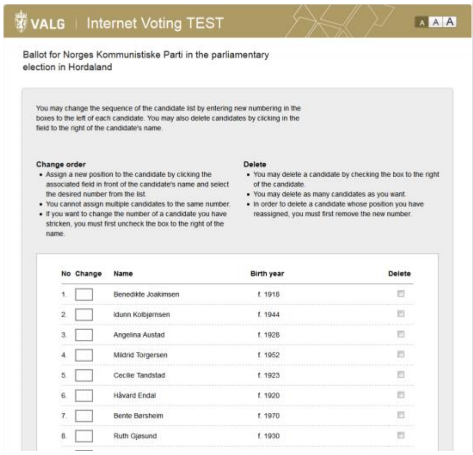
Select ballot for parliamentary election in Hordaland

There are 15 electoral lists in your county. These are listed in random order below. Choose the party you want to vote for.

○ Norges Kommunistiske Parti
○ Pensjonistpartiet
○ Det norske Arbeiderparti
○ Miljøpartiet De Grønne
○ Sentrumsalliansen
○ Rødt
○ Demokratene
○ Fremskrittspartiet
○ Sosialistisk Venstreparti
○ Kystpartiet
○ Venstre
○ Senterpartiet
○ Høyre
○ Kristent Samlingsparti
○ Kristelig Folkeparti

○ Blank stemmeseddel

Show ballot



Ballot for Norges Kommunistiske Parti in the parliamentary election in Hordaland

You may change the sequence of the candidate list by entering new numbering in the boxes to the left of each candidate. You may also delete candidates by clicking in the field to the right of the candidate's name.

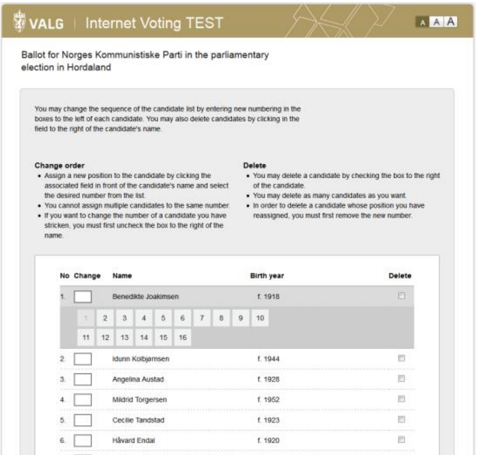
Change order

- Assign a new position to the candidate by clicking the associated field in front of the candidate's name and select the desired number from the list.
- You cannot assign multiple candidates to the same number.
- If you want to change the number of a candidate you have stricken, you must first uncheck the box to the right of the name.

Delete

- You may delete a candidate by checking the box to the right of the candidate.
- You may delete as many candidates as you want.
- In order to delete a candidate whose position you have reassigned, you must first remove the new number.

No	Change	Name	Birth year	Delete
1.	□	Benedikte Joakimsen	f. 1918	□
2.	□	Idunn Kolbjørnsen	f. 1944	□
3.	□	Angelina Austad	f. 1928	□
4.	□	Mildrid Torgersen	f. 1952	□
5.	□	Cecilie Tandstad	f. 1923	□
6.	□	Håvard Endal	f. 1920	□
7.	□	Bente Børsheim	f. 1970	□
8.	□	Ruth Gjøsund	f. 1930	□



Ballot for Norges Kommunistiske Parti in the parliamentary election in Hordaland

You may change the sequence of the candidate list by entering new numbering in the boxes to the left of each candidate. You may also delete candidates by clicking in the field to the right of the candidate's name.

Change order

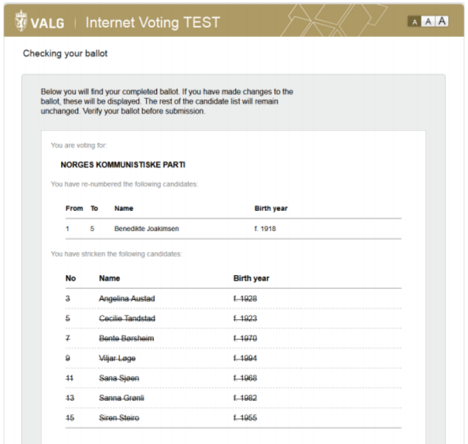
- Assign a new position to the candidate by clicking the associated field in front of the candidate's name and select the desired number from the list.
- You cannot assign multiple candidates to the same number.
- If you want to change the number of a candidate you have stricken, you must first uncheck the box to the right of the name.

Delete

- You may delete a candidate by checking the box to the right of the candidate.
- You may delete as many candidates as you want.
- In order to delete a candidate whose position you have reassigned, you must first remove the new number.

No	Change	Name	Birth year	Delete
1.	□	Benedikte Joakimsen	f. 1918	□
	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16			
2.	□	Idunn Kolbjørnsen	f. 1944	□
3.	□	Angelina Austad	f. 1928	□
4.	□	Mildrid Torgersen	f. 1952	□
5.	□	Cecilie Tandstad	f. 1923	□
6.	□	Håvard Endal	f. 1920	□

[11] [NC1]"Can we trust internet voting? Internet voting in Norway", Henrik Nore, The Ministry of Local Government and modernization, ONPE-OAS Lima, Oct 22, 2013



VALG | Internet Voting TEST

Checking your ballot

Below you will find your completed ballot. If you have made changes to the ballot, these will be displayed. The rest of the candidate list will remain unchanged. Verify your ballot before submission.

You are voting for:

NORGES KOMMUNISTISKE PARTI

You have re-numbered the following candidates:

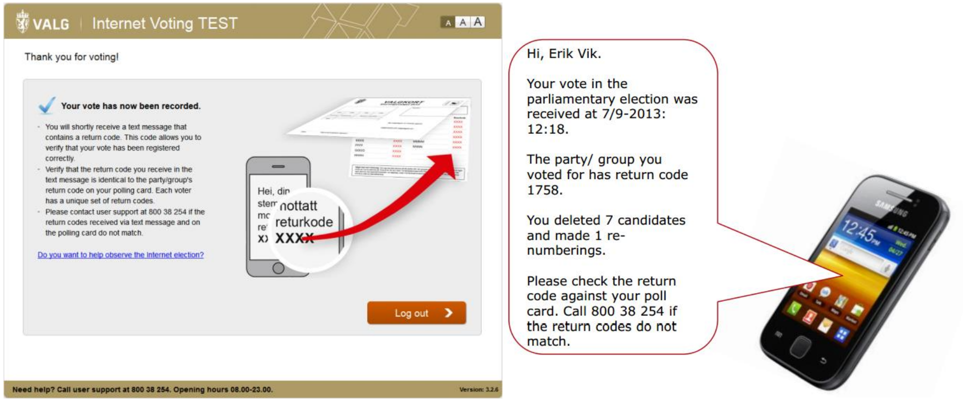
From	To	Name	Birth year
1	5	Benedikte Joakimsen	f. 1918

You have stricken the following candidates:

No	Name	Birth year
~~3~~	~~Angelina Austad~~	~~f. 1928~~
~~5~~	~~Cecilie Tandstad~~	~~f. 1923~~
~~7~~	~~Bente Børsheim~~	~~f. 1970~~
~~9~~	~~Viljar Løge~~	~~f. 1994~~
~~11~~	~~Sana Sjøen~~	~~f. 1968~~
~~13~~	~~Sanna Grønli~~	~~f. 1982~~
~~15~~	~~Siren Steiro~~	~~f. 1955~~

Figure 2: Demonstration of the Voting Process [NC1, p28-36]

- After submitting a vote, voters can verify his/her preference is correctly recorded via the return code sent to their mobile phone, by comparing this return code with the one printed on their polling card.



VALG | Internet Voting TEST

Thank you for voting!

Your vote has now been recorded.

- You will shortly receive a text message that contains a return code. This code allows you to verify that your vote has been registered correctly.
- Verify that the return code you receive in the text message is identical to the party/group's return code on your polling card. Each voter has a unique set of return codes.
- Please contact user support at 800 38 254 if the return codes received via text message and on the polling card do not match.

Do you want to help observe the Internet election?

Need help? Call user support at 800 38 254. Opening hours 08.00-23.00.

Hi, Erik Vik.

Your vote in the parliamentary election was received at 7/9-2013: 12:18.

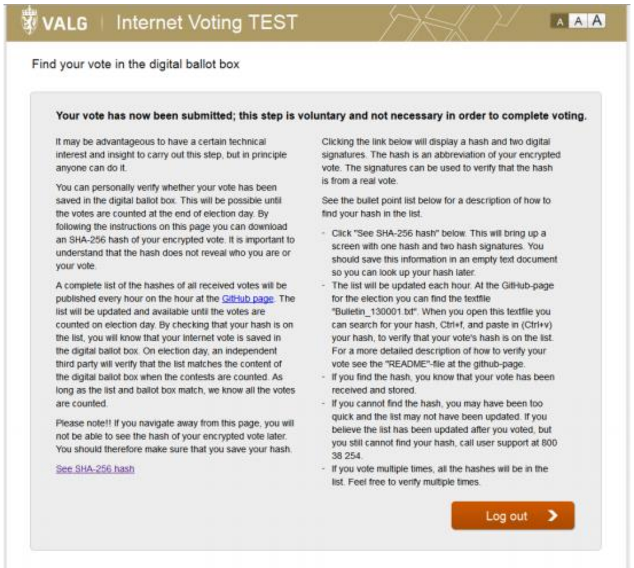
The party/ group you voted for has return code 1758.

You deleted 7 candidates and made 1 re-numberings.

Please check the return code against your poll card. Call 800 38 254 if the return codes do not match.

Figure 3: Use of the Return Code in voter verification [NC1, p38-40]

- In addition, the voter can verify the preference is correctly recorded in the digital vote box by comparing hash value of their votes with the hash in the public bulletin board list file to see whether or not it matches.



Find your vote in the digital ballot box

Your vote has now been submitted; this step is voluntary and not necessary in order to complete voting.

It may be advantageous to have a certain technical interest and insight to carry out this step, but in principle anyone can do it.

You can personally verify whether your vote has been saved in the digital ballot box. This will be possible until the votes are counted at the end of election day. By following the instructions on this page you can download an SHA-256 hash of your encrypted vote. It is important to understand that the hash does not reveal who you are or your vote.

A complete list of the hashes of all received votes will be published every hour on the hour at the GitHub page. The list will be updated and available until the votes are counted on election day. By checking that your hash is on the list, you will know that your Internet vote is saved in the digital ballot box. On election day, an independent third party will verify that the list matches the content of the digital ballot box when the contests are counted. As long as the list and ballot box match, we know all the votes are counted.

Please note!! If you navigate away from this page, you will not be able to see the hash of your encrypted vote later. You should therefore make sure that you save your hash.

See SHA-256 hash

Clicking the link below will display a hash and two digital signatures. The hash is an abbreviation of your encrypted vote. The signatures can be used to verify that the hash is from a real vote.

See the bullet point list below for a description of how to find your hash in the list.

- Click "See SHA-256 hash" below. This will bring up a screen with one hash and two hash signatures. You should save this information in an empty text document so you can look up your hash later.
- The list will be updated each hour. At the GitHub-page for the election you can find the textfile "Bulletin_130001.txt". When you open this textfile you can search for your hash, Ctrl+f, and paste in (Ctrl+v) your hash, to verify that your vote's hash is on the list. For a more detailed description of how to verify your vote see the "README"-file at the github-page.
- If you find the hash, you know that your vote has been received and stored.
- If you cannot find the hash, you may have been too quick and the list may not have been updated. If you believe the list has been updated after you voted, but you still cannot find your hash, call user support at 800 38 254.
- If you vote multiple times, all the hashes will be in the list. Feel free to verify multiple times.

Figure 4: Instruction on How to verify votes in the digital vote box [NC1, p39]

- After the election is closed, the Internet Election Committee (IEC) will provide their shares of the private decryption key to the Decryption / Counting Service. The Decryption / Counting Service decrypt the votes and generate a zero-knowledge proof of correct decryption. After the auditor has verified the proof, the votes are counted and the result is published.

2. Security & Trust

2.1 Security:

The cryptographic protocol used in Norway is a fairly standard internet voting system based on ElGamal encryption of ballots and a mix-net before decryption. The voter gives his ballot to a computer, which encrypts the ballot and submits it to a ballot box. The ballot box and a return code generator cooperate to compute a sequence of return codes for the submitted ballot. These codes are sent by SMS to the voter's mobile phone. The voter verifies the return codes against a list of pre-computed return code pairs printed on his voting card. Once the ballot box closes, the submitted cipher texts are decrypted by a decryptor. An auditor supervises the entire process and will be able to verify the integrity of the tally. More details of the cryptographic protocol can be found in [NC2] “The Norwegian Internet Voting Protocol”

The MLGRD hired mnemonic to perform a source code audit to “review those parts of the EVA that implement cryptographic primitives and generate keys”. According to the technical report, mnemonic has not discovered any critical cryptographic weakness that would preclude the use of the Internet voting system. The most serious technical issue discovered is an error in an encryption format for storing password protected data. To see detailed discussion of flaws and potential security issues uncovered by the audit, refer to [NC3]

Other security related questions can be found in Table 2.

2.2 **Trust Structure:**

Issue	Summary Answers
Whom (or what equipment & processes) must the voter trust that: • the correct blank ballot is delivered with all races and issues present?	• Key Management Service • Printing service • Postal service
• their choices (candidates and/or issues) are recorded correctly before the marked ballot leaves their device?	• Voter computer • Internet • Return Code Generator
• their ballot as been received by local election office?	• Vote Collector Service • Internet • Key Management Service
• that their ballot has been a part of the tabulation?	• Mix-Net
• that their ballot choices have been tallied correctly in the total cast ballots results?	• Electoral Roll Service • Decryption/ courting service • LEO • Auditors
Whom must the local election official trust	• Vote collector service • Key management service

• that the ballot presents the correct ballot choices for a given voter?	
Whom must voter & general public trust that the votes have been tallied & reported to the public correctly?	• LEO • Auditor • Electoral Roll Service • Key Management Service

2.3 Dispute Resolution

Insufficient Information.

2.4 Documented Security Issues and Hacks

On 5 September, the MLGRD discovered that the Internet voting client software contained a programming error causing weak encryption of some 29,000 electronic votes, potentially jeopardizing the secrecy of those votes. The MLGRD sufficiently addressed the issue by correcting the client software and tightening the access restrictions to the electronic ballot box. [NC4 p4]

In addition, there were a number of Internet votes cast which were invalid (9 votes) or rejected (1 vote) during the election. In the case of the invalid votes, the recorded preferences were invalid because more than one vote was recorded for a party list. The rejected ballot was received just before the end of the 30 minute voting session time limit, but so close to the end that it was processed just after the end of the 30 minute period and was rejected during the cleansing phase of the counting process.

In both cases voters casting these ballots received a return code and were informed by the voting application that their votes had been successfully submitted.

Despite the small number of ballots involved, the extemporaneous ballot clearly represents a failure because the system wrongly informed the voter that his/her vote had been successfully cast. [NC5, p74]

> Scytl, the Internet voting solution provider, investigated how such invalid ballot choices were possible and concluded that “it could either have been a successful attempt to manipulate the system or an error in the voting applet allowing invalid choices to be submitted.” [NC5, p88]

3. Auditability

The Norwegian Internet voting system has made significant efforts to provide a system which is auditable, and provides mechanisms for stakeholders to independently check the correct functioning of the system.

The Ministry decided to contract an outside independent organization, Promis AS, to conduct verification functions for the Internet voting system, including the verification/audit of the processing of ballots received on the VCS through the counting and results process.

In addition, every event on infrastructure components and transactions on the various servers used by the Internet voting system (such as the VCS, RCG, cleansing server, mixing server and tabulation server) was logged using immutable logs. These logs were monitored by the Ministry using a professional log monitoring system as the project unfolded, and were also reviewed through a comprehensive post-election audit. Ongoing monitoring of the functioning of the infrastructure also took place, with alerts sent to key staff when issues of concern arose. However, there were concerns on the openness of the audit processing, which should be an area for future improvement.

This section is predominantly drawn from IFES’s assessment on Norway E-vote Project’s Compliance with International Standards, refer to [NC4] for detailed narrative.

4. Vote Privacy, s*ee System Details Table.*

5. Testing and Deployments: for Performance/Functionality and Security, s*ee System Details Table.*

6. Usability & Accessibility Assessments (including testing for these attributes), s*ee System Details Table.*

7. **Infrastructure Requirements and Potential Costs**, s*ee System Details Table*.

Group III Systems

Democracy Live

Introduction:

“The Democracy Live suite of electronic balloting tools is called Live Ballot. Live Ballot. has been deployed in hundreds of U.S. elections and used by U.S. military and overseas voters in 96 countries and every continent in the world.”[1] Democracy Live claims to be the most deployed web based ballot system on the market today. They also claim that their system “...has been deployed in hundreds of elections and used by U.S. military voters, disabled voters, remote voters and domestic voters looking for their specific ballot and balloting information.”[1]

Core Architecture & Operation:

The core of the system is Live Ballot. Live Ballot. is a closed-source Internet voting system which has been used in a variety of different hasn't

Security & Trust:

They have claimed to have top level security that prevents fraud but outside of experts that they claim have validated the system, there hasn't been any other third parties available to validate those claims.

References:

- "ELECTRONIC BALLOTING." Democracy Live Inc. N.p., n.d. Web. 17 Apr. 2014.
- <http://democracylive.com/>.

Everyone Counts (E1C)

0. Introduction:

Everyone Counts is one of the major remote voting technology providers in the United States, operating on the "Software as a Service" (SaaS) and commercial, off-the-shelf (cots) hardware model. Everyone Counts (E1C) has been widely deployed within United States and worldwide, both public and private sectors. The list of organizations that deployed the systems is available at https://everyonecounts.squarespace.com/case-studies/overview/

E1C's latest voting system is called eLect, which is an integrated Election Administration and Voting system that claims to be "Scalable, Sustainable, Efficient, Accurate, Secure, Accessible, Auditable, Cost-Effective."[12] Everyone Counts adopted the Open Code Advantage policy, which allow the client to audit the system, perform penetration test, review the source code and review the cryptography.

1. Core Architecture & Operation

1.1 Basic Architecture & Design;

Due to the fact that the eLect system can be integrated partially and remodeled flexibly according the Election Committee's requirements, we will limit our discussion to the standard design of the system in the report.

The standard eLect system consists of voter registration, Candidate filing, pre-voting administration, voting, post-voting administration, tabulation and reporting. Refer to figure 1 for specific features within each component.

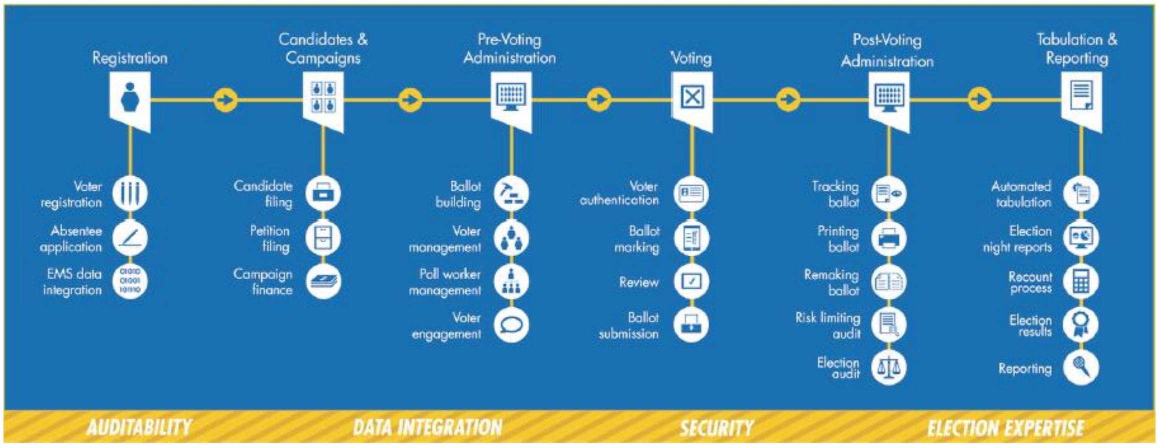


Figure1: eLect system voting system components[13]

[12] [E1C1] "Introduction to eLect system", Everyone Counts, http://www.everyonecounts.com/introduction-to-elect/

[13] [E1C2, p6] "Request for Information: Uniform Voting System for the State of Colorado", Everyone Counts Inc. April 1, 2013

2. Security & Trust

2.1 Security

The vendor claimed that eLect system adopted “military-grade security and accredited, industry-standard data hosting and storage facilities”[14]. The cryptographic protocol includes encryption method such as Secure Socket Layer (SSL), AES, RSA and 3DES.

The data centers is equipped with physical security and access control, the database has implemented firewall controls and intrusion protection, antivirus and malware controls, system hardening best practices, detecting and reporting principles.

Everyone Counts claimed to adhere to the National Institute of Standards and Technology’s (NIST) guidelines for encryption, threat modeling, physical server security, and tamper-detection monitoring.[15]However, we could not found any public available security auditing, assessment or certification of the eLect system.

2.2 Trust Structure

Voters need to trust the eLect software to correctly record their voting preference. Everyone Counts is currently using Quad Audit for verification and auditing purpose. Although this sounds like a strong verifiability solution, it is still vulnerable when the server was hacked or manipulated so that the "receipt "would appear to work well but the votes were tampered. This indicates that voters also need to trust the server for their votes to be cast as recorded and tallied as recorded.

2.3 Documented Security Issues

In the case of New South Wale's iVote system, where Everyone Counts served as the technical provider, it was reported that the iVote system mis-recorded 43 votes due to a software bug in input validation. The bug is only detected by the Election Committee because the votes it produced were invalid, which indicates that this malfunction would have been undetected if it produced valid votes.

Based on the architecture and design of the system, it is possible that eLect system could be exploited by SSL vulnerabilities (such as Heart bleed), and other known Cloud Computing and COTS vulnerabilities.

[14] [E1C 1]

[15] [E1C 2, p21]

3. Auditability

Everyone Counts is currently using Quad Audit for auditing purpose. The electronically cast ballot can be saved in the following four ways:

- Paper ballot with text
- 2D/QR code of ballot selections printed in the corner of the paper ballot
- Encrypted ballot image
- Encrypted electronic ballot[16]

To ensure this auditability, the election committee must use Everyone Counts for the full end-to-end voting solution. Everyone Counts can integrate with other vendors, but it would increase the cost and we cannot guarantee complete auditability.[17]

4. Voter Privacy

Voter privacy issue is somewhat mitigated by eliminating voter identification information. It is stated that only the votes will be stored on the electronic ballot, the paper ballot, as well as the bar code printed in the corner of the paper ballot, therefore avoiding revealing voter identification information during both casting and auditing process.

5. Testing & Deployments

eLect source code has been reviewed and accredited by the following their party organizations: New South Wales Electoral Commission, United States Business Transformation Agency, Florida Department of States, Wyle Laboratories, SLI Global Solutions, BMM Compliance, Netcraft, PWC and Red Phone Security. [18]

In the case of New South Wale iVote system, where PWC is engaged in auditing the system, there are limitation of the testing and evaluation process that raises concerns:

- The audit was performed in a short time frame
- Neither the pre audit or the post audit report documents details of the identified vulnerabilities
- The qualification of the auditors and other parties involved in the evaluation process is questionable

[16] [E1C 1]

[17] [E1C 2, p30]

[18] [E1C 3] “Submission to the Inquiry into the future of Victoria’s electoral administration”, Everyone Counts, Feb 1, 2013

- Week transparency and lack of openness to scrutiny: Open Code Advantage policy doesn't not apply to any interested third party [19]

6. Usability

At this stage, there is no independent usability report found on Everyone Count's eLect system. (It is possible that there are usability aspects of the assessment with Systems that adopted Everyone Count's technology. Need further examination)

Everyone Counts has cooperated with various groups to study and enhance the accessibility for people with disabilities. Everyone counts partnered with The University of Colorado Anschutz Medical Campus and Assistive Technology Partners (ATP) in a research program designed to study assistive technologies for voters with disabilities. In October 2012, Everyone Counts published a white paper detailed case studies and current practices for providing and improving voting access and participation by persons with disabilities.[20]

Everyone counts provided accessibility options include "telephone voting solution, integration a variety of reading tools for audio ballot capabilities, Bluetooth devices, and sip-and-puff devices"[21].

7. Infrastructure & Cost

Equipment needed by the vote: Electronic voting units including PCs, tablets or smartphones

Equipment needed by the local election officials varies substantially based on their current capability and local election regulations.

Combining the benefits of Commercial Off-the-Shelf (COTS) hardware and its Software-as-a-Service (SaaS) model, Everyone Counts claims that they can reduce 20 -50% in the costs comparing to traditional election systems and processes. [22]

"By choosing Everyone Counts' secure, easy-to-use solution, we have saved significant time and money on this election by streamlining the administrative process and cutting over 50% of the costs for mailing and other expenditures." Joan Manke, Executive Director, Honolulu Neighborhood Board Commission

[19] [E1C 4] "Problems with the iVote Internet Voting System", Venessa Teague and Roland Wen, 2011

[20] [E1C 5] "Increasing Accessibility to Voting with New Technology", An Everyone Counts White Paper, September 2012

[21] [E1C 2, p25]

[22] [E1C 6] "Submission to the Inquiry into the 2012 Local Government Elections", Everyone Counts, Aug. 2, 2013

iOASIS

Introduction:

“The iOASIS system was developed and tested more than 1,000 times by the South Dakota National Guard as well as a number of overseas military bases. Intended as way to streamline absentee voting for military members serving overseas, it utilizes technology from the DoD such as the Common Access Card (CAC).”[1]

Core Architecture & Operation:

““iOASIS is based on a concept of simplicity,” said Gant. These voters will now be able to register to vote, request an absentee ballot, receive an absentee ballot and mark an absentee ballot in seconds. The ballot is then printed and returned for counting. This is only possible by utilizing the security of the Common Access Card for validation to verify our overseas voters and turn a 60-day process into a less than 5-minute transaction.””[1]

Security & Trust:

The only security that has been advertised for the system is the use of the common access card. This card would be used to validate the user and prove (on top of other identification) that the voter is who they say they are. Outside of this, there is no additional information on the security and trust.

Future:

iOASIS was launched Tuesday, March 25, 2014 to great reviews.

References:

- GSN. "South Dakota Secretary of State Activates IOASIS Computerized Military Voting System." Government Security News. GSN, 28 Mar. 2014. Web. 16 Apr. 2014. <http://www.gsnmagazine.com/article/40653/south_dakota_secretary_state_activates_ioasis_comp>.
- Plyler, Kim. "IOASIS to Streamline Voting Process for Overseas Personnel." Scoop. Scoop World, 27 Mar. 2014. Web. 16 Apr. 2014. <http://www.scoop.co.nz/stories/WO1403/S00335/ioasis-to-streamline-voting-process-for-overseas-personnel.htm>.

Arizona

0. Introduction

Arizona became the first state to offer internet voting for a national election to overseas military and civilians through a central website. Internet voting is available for overseas military and civilian families as well. This system does not qualify as an end-to-end verifiable because there is no process of integrity or verifiability for the voting process, record, cast, and tally.

1. Core Architecture & Design

1.1 Basic Architecture & Design,

The system designed for overseas voters first requires registration through a Secretary of State website. Once registered a ballot is either mailed or emailed to the voter as a PDF. When the ballot is received the voter prints it out and marks their ballot choice. The completed and signed ballot is then scanned into a personal computer and uploaded to a secure system using SSL encryption (2). Once received by the election official the ballot is printed and process as a traditional absentee ballot.

2. Security & Trust

2.1 Security

The system used for overseas voting relies on email which is inherently insecure. Several threats include man in the middle attacks, phishing attacks, and malware infection of voter computers, which could compromise the integrity of a ballot (2).

3. Future

The system is still available to residents of Arizona. With the increasing state-sponsored cyber-attacks against government agencies and financial institutions the potential threats to Internet elections which lack the ability to recovery available to financial institutions is a considerable risk (3). A prominent computer network security expert Bruce Schneier put it this way, “If there’s electronic banking fraud, we look at what happens, we can roll it back and make everybody whole. We can’t do that with a voting system.” (3).

Sources

(1) http://www4.nau.edu/srl/PressReleases/99f%20-%20Internet%20Voting.pdf

(2) http://www.wired.com/2009/06/cfp-evote/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+wired27b+(Wired%253A+Blog+-+Threat+Level)

(3) http://thevotingnews.com/lawmaker-seeks-pilot-program-to-test-online-voting-in-arizona-cronkite-news/

Alaska

Introduction:

“In 2012, Alaska selected an on-line ballot delivery solution to offer an electronic voting alternative to all absentee voters.”[1] Through these pursuits Alaska teamed up with SOE (Scytl) to develop an on-line voting system to be used by uocava and absentee voters. The system is currently deployed and is in use by the states citizens.

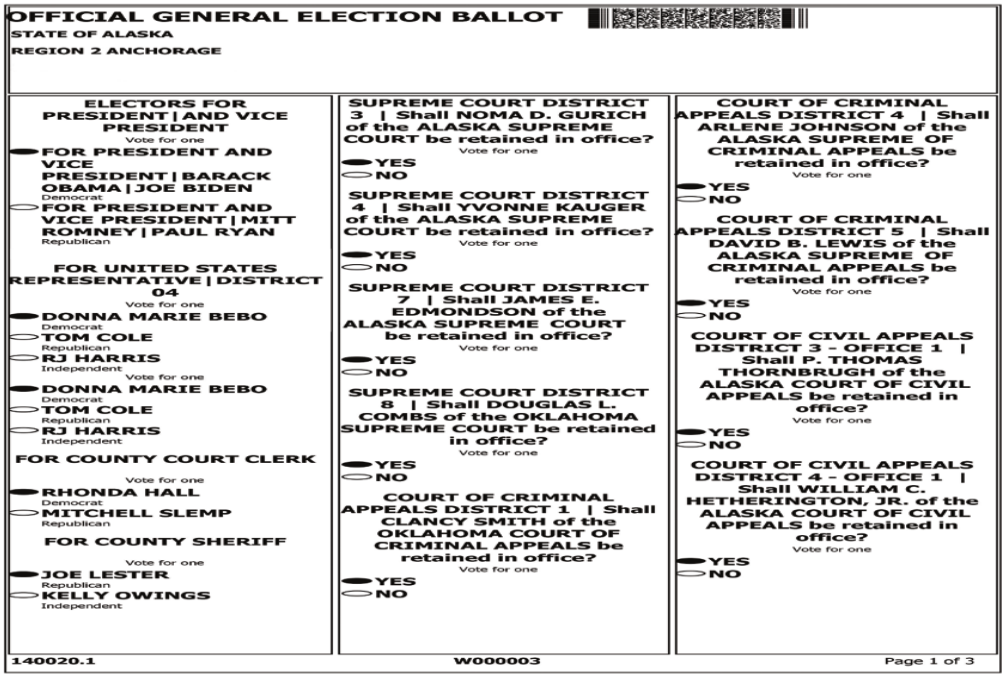
Core Architecture & Operation:

“The online ballot delivery system is an electronic ballot transmission and onscreen marking tool specifically designed to fulfill the requirements of the MOVE Act. It is a web application that enables all absentee voters in the State of Alaska to to securely receive and return their ballots online while preserving the integrity and privacy of their vote.”[sic][1] The system itself is a simple web portal that allows for qualified users to log in, verify their identity and then vote as an absentee.

Security & Trust:

Very little was spoken of the security of the system but they have claimed that they are secure and have been tested by a third party. That being said, the voting system's security is still up for debate as no other reports have been published publicly and the system is not open source.

Pictures:



OFFICIAL GENERAL ELECTION BALLOT
STATE OF ALASKA
REGION 2 ANCHORAGE

ELECTORS FOR PRESIDENT | AND VICE PRESIDENT
Vote for one
● FOR PRESIDENT AND VICE PRESIDENT | BARACK OBAMA | JOE BIDEN
Democrat
○ FOR PRESIDENT AND VICE PRESIDENT | MITT ROMNEY | PAUL RYAN
Republican

FOR UNITED STATES REPRESENTATIVE | DISTRICT 04
Vote for one
● DONNA MARIE BEBO
Democrat
○ TOM COLE
Republican
○ RJ HARRIS
Independent
Vote for one
● DONNA MARIE BEBO
Democrat
○ TOM COLE
Republican
○ RJ HARRIS
Independent

FOR COUNTY COURT CLERK
Vote for one
● RHONDA HALL
Democrat
○ MITCHELL SLEMP
Republican

FOR COUNTY SHERIFF
Vote for one
● JOE LESTER
Republican
○ KELLY OWINGS
Independent

SUPREME COURT DISTRICT 3 | Shall NOMA D. GURICH of the ALASKA SUPREME COURT be retained in office?
Vote for one
● YES
○ NO

SUPREME COURT DISTRICT 4 | Shall YVONNE KAUGER of the ALASKA SUPREME COURT be retained in office?
Vote for one
● YES
○ NO

SUPREME COURT DISTRICT 7 | Shall JAMES E. EDMONDSON of the ALASKA SUPREME COURT be retained in office?
Vote for one
● YES
○ NO

SUPREME COURT DISTRICT 8 | Shall DOUGLAS L. COMBS of the OKLAHOMA SUPREME COURT be retained in office?
Vote for one
● YES
○ NO

COURT OF CRIMINAL APPEALS DISTRICT 1 | Shall CLANCY SMITH of the OKLAHOMA COURT OF CRIMINAL APPEALS be retained in office?
Vote for one
● YES
○ NO

COURT OF CRIMINAL APPEALS DISTRICT 4 | Shall ARLENE JOHNSON of the ALASKA SUPREME OF CRIMINAL APPEALS be retained in office?
Vote for one
● YES
○ NO

COURT OF CRIMINAL APPEALS DISTRICT 5 | Shall DAVID B. LEWIS of the ALASKA SUPREME OF CRIMINAL APPEALS be retained in office?
Vote for one
● YES
○ NO

COURT OF CIVIL APPEALS DISTRICT 3 - OFFICE 1 | Shall P. THOMAS THORNBRUGH of the ALASKA COURT OF CIVIL APPEALS be retained in office?
Vote for one
● YES
○ NO

COURT OF CIVIL APPEALS DISTRICT 4 - OFFICE 1 | Shall WILLIAM C. HETHERINGTON, JR. of the ALASKA COURT OF CIVIL APPEALS be retained in office?
Vote for one
● YES
○ NO

140020.1 W000003 Page 1 of 3

References:

- SOE/Scytl. THE STATE OF ALASKA ONLINE BALLOT DELIVERY AND RETURN. Tech. SOE Election Management, 12 Feb. 2014. Web. 17 Apr. 2014. <http://www.nass.org/component/docman/?task=doc_download&gid=1508&Itemid=>.

Maryland

Introduction:

Maryland has been seeking to pioneer an online ballot marking system that was designed through a contractual development process. “In 2001, the Maryland General Assembly passed a law that required the State Board of Elections, in consultation with the local boards of elections, to select and certify a uniform, statewide voting system.”[1] Because this law, Maryland decided to use a standard electronic voting system implemented throughout the state developed by ESS Inc. The online ballot marking system was created but it was unable to be deployed due to security problems and inefficient testing by unreliable testers.

Core Architecture & Operation:

“For polling place voting, voters use a touchscreen voting system by Election Systems and Software Inc (formerly Premier Election Solutions), the AccuVote-TS. With a touchscreen voting system, a voter touches the screen to make, change, and review selections and cast a ballot.”[1] The AccuVote-TS is an electronic voting system that uses a touchscreen interface. The online ballot marking system that was developed for military, overseas citizens and disabled voters allows for electronically deliver ballots that could be printed, filled out and sent back to the proper officials.

Security & Trust

“Maryland’s voting units and central tabulator are never connected to the Internet. Voting units are sealed from the time the ballots are loaded until election judges open them on election day morning. Tamper tape is used to deter unauthorized access and alert election officials of possible tampering. Votes are stored in two different places on each voting unit. Unofficial election results sent via modem on election night are not part of the official results. Official election results are loaded from the memory cards the day after the election.”[1] Maryland claims that their system has been reviewed more than any other system making them the most secure system in the country.[1]

When it comes to the online ballot marking system it does not the industry standards of security. One of the problems with the system is that it wasn't tested properly. “...board members were troubled by an IT security assessment conducted for the state by a firm that has never performed Internet security tests on election systems. The Largo-based company, Unatek, Inc., also didn’t study voter fraud risks at the front end of the voting system where ballots are requested online.”[4] This resulted in the system appearing to be safe but further research prove otherwise. In the paper “Risks Presented by On-Screen and Online Electronic Ballot Marking” by David Jefferson and Candice Hoke, they highlighted a number of vulnerabilities that plague the Maryland's online ballot marking system. These problems range from the vulnerabilities of electronic ballot marking to the inherent privacy flaws and the limitation of testing and certifications. All of which make the system strategically flawed and insecure, calling to question the validity of its use or even its existence.[3]

Future

Maryland will move back to paper ballots in time for 2016 elections.[2]

Reference

- Maryland. "Overview of Maryland's Voting System." Voting System Overview. Maryland, n.d. Web. <http://www.elections.state.md.us/voting_system/index.html>.
- Kazanjian, Glynis. "MarylandReporter.com." Maryland Prepares Move Back to Paper Ballots for Elections. Maryland Reporter, 19 Nov. 2013. Web. <http://marylandreporter.com/2013/11/19/maryland-prepares-move-back-to-paper-ballots-for-elections/>.
- Jefferson, David, and Candice Hoke. Risks Presented by On-Screen and Online Electronic Ballot Marking. Security Review. N.p.: n.p., n.d. Print.
- Kazanjian, Glynis. "Online Ballot Tool Goes Uncertified over IT Security Concerns." Local News ATOM. Cumberland Time News, 28 Apr. 2014. Web. 01 May 2014. <http://www.times-news.com/local/x493481867/Online-ballot-tool-goes-uncertified-over-IT-security-concerns>.

Scytl (Group 3)

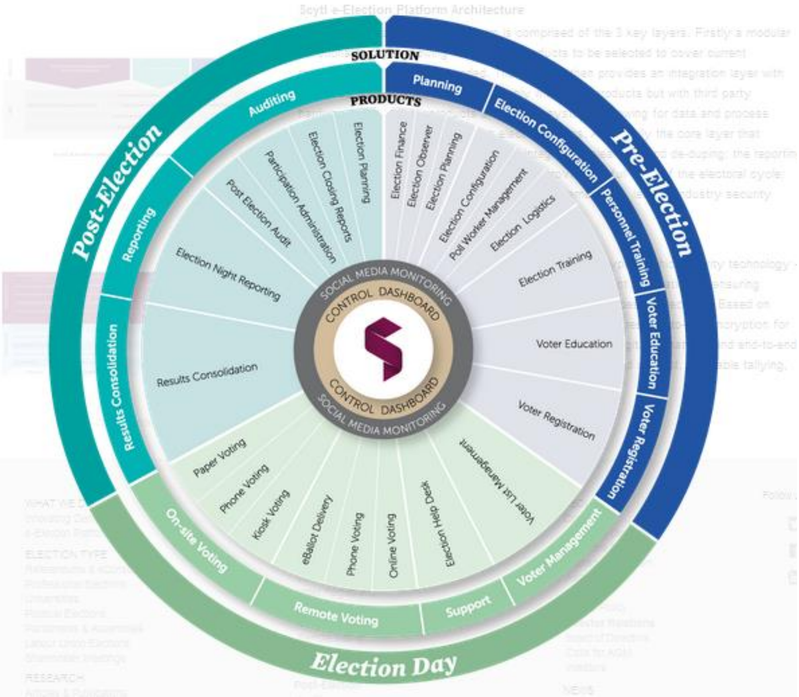
0. Introduction:

Scytl is a Spain based privately owned company providing secure election management and electronic voting solutions. Specializing in election modernization technologies, Scytl's e-Election platform incorporates unique cryptographic protocols that ensure maximum security, transparency and auditability in all types of elections. Founded in 2001 as a spin-off from a university research group, Scytl has a strong focus on R&D. Scytl's solutions have been deployed in 35 countries throughout the world over the last 10 years, including Canada, the United States, Mexico, Ecuador, France, Norway, Switzerland, Bosnia-Herzegovina, the UAE, India, Iceland and Australia. Scytl is headquartered in Barcelona, with strategic offices the United States, Canada, Brazil, Peru and Greece as well as field offices in the UK, Ukraine, Malaysia, India and Australia.[23]

1. Core Architecture & Operation

1.1 Basic Architecture & Design;

Similar to Everyone Counts, Scytl's e-Election platform offers products and services through the full election cycle from pre-election to election day to post-election.(See Figure 1 for details)



[23] Company Overview, Scytl, http://www.scytl.com/company-overview/

Figure 1: e-Election Platform overview[24]

The platform is composed with 3 key layers: 1) a modular functionality layer 2)an integration layer consolidate with third party hardware and software, as well as legacy items 3)the core layer that leverages database, the reporting engine and the security framework layer.[25]

2. Security & Trust

2.1 Security:

Scytl's internet voting system is referred as Pnyx. The newest version of Pynx was launched in August 2011. Due to the limitation in public available resource, the project team could only find security assessment of Pnyx dated before 2011. Therefore, this section may not address the new addition features of the voting system.

Cryptographic primitives the system adopted include RSA encryption, RSA digital signatures, 3DES encryption in CBC mode. In addition, Scytl use their own design of cryptographic protocols through the voting and mixing (a decryption service) process.[26]

2.2 Trust Structure:

In general, significant amount of trust needs to be placed on Vendor voting system, vendor server as well any third party hardware and software that vendor choose to include, through the full election cycle.

Detail see Metrics

2.3 Dispute Resolution - no information available

2.4 Documented Security Attacks and Security Issues

- In 2008, the Florida Department of State commissioned a review of Scytl's remote voting software and concluded, in part, that:
  - *The system is vulnerable to attack from insiders.*
  - *In a worst case scenario, the software could lead to (1) voters being unable to cast votes; (2) an election that does not accurately reflect the*

[24] http://www.scytl.com/e-election-platform/

[25] Ibid.

[26] [SCY1, p50]

  will of the voters; and (3) possible disclosure of confidential information, such as the votes cast by individual voters.
  - *The system may be subject to attacks that could compromise the integrity of the votes cast.*[27]

  Still, the Florida Department of State provided SCYTL with a Provisional Certification valid for two years certifying the company was "deemed compliant with the functional and security requirements." [28]
- In 2010, Scytl's ePollBook was deployed in Washington, D.C.. Prior to deploying the system in the general election, a public trial was conducted. A team of researchers in University of Michigan Ann Arbor participated in this trial. Within 48 hours of the system going live, they were able to gain near complete control of the election server. They successfully changed every vote and revealed almost every secret ballot, without Election Official's detection for two days.[29] A case study of their experience is published in Feb 2012.
- During the 2012 Canada New Democratic Party's Leader Election, a Distributed Denial of Service attack (DDoS) occurred, causing delay by several hours and left many delegates unable to cast their ballots. At the time, neither the NDP, nor Scytl, explain beyond saying it was a denial of service attack. On March 2014, Scytl announced that "the problem stemmed from a link on the New Democrats' website that directed members to Scytl's secure website, allowing the denial of service attack to hit a public page".[30]
- In 2013, Scytl system is deployed in Ecuador Sectional elections, for the vote processing, automated tally and publication of electoral results. "Eight days after Election Day, Scytl stated there were problems in the system", leading to the delays in processing the electoral records as well as announcing the official results. Scytl has publicly accepted its failure in Ecuador, and stated it is caused by their technicians.[31]
- Scytl used OpenSSL which raises concern that the voting system might be vulnerable to the recent revealed Heartbleed bug. On Apr 10 2014, Scytl stated in the new release that all its voting implements are not affected by Hearbleed due to its "full and in-depth end-to-end encryption and security" The specific

[27] [SCY1]Software Review and Security Analysis of Scytl Remote Voting Software, Michael Clarkson, Brian Hay, Meador Inge abhi shelat, David Wagner, Alec Yasinsac, September 19, 2008

[28] [SCY2] http://kleinonline.wnd.com/2012/10/26/confirmed-spanish-firm-to-provide-overseas-military-ballots-absentee-voter-requests-currently-down-by-staggering-numbers/

[29] [SCY3] Attacking the Washington, D.C. Internet Voting System, Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012

[30] [SCY4]http://www.cbc.ca/news/politics/ndp-site-the-weak-link-in-online-attack-during-2012-leadership-vote-1.2557861

[31] [SCY5]http://digitalvote.wordpress.com/tag/electronic-voting-pilot-test-scytl/

reasons include: 1) Scytl does not use the specific OpenSSL code library (1.0.1) that is affected; 2) votes are encrypted on the client devise where the voting takes place 3) its authentication mechanism prevent attackers to obtain passwords as they are not sent via communication channel. [32] Though immune from Heart bleed, we can still conclude that Scytl's voting system is subject to known OpenSSL vulnerabilities.

3. Auditability

With Scytl Online Voting, voters are provided with a voting receipt that contains a unique identifier that enables voters to check that their votes have reached the Electoral Board and have been counted. The random nature of Scytl's voting receipt impedes the disclosure of the ballot choices selected. [33]However, because the receipts are unrelated to the choices made by voters on their ballots, it can't be seen as a proof of cast as intended. In addition, if the system doesn't function as intended, the receipts do not guarantee that votes were cast and tallied accurately.[SCY1, p63]

Scytl's utilize its patent proprietary technology named "Immutable logs" to prevents log files integrity,

[32] [SCY6]http://www.scytl.com/news/scytl-security-protocols-ensure-clients-unaffected-heartbleed-bug/

[33] Voter self verification, Scytl, http://www.scytl.com/products/election-day/scytl-online-voting/

Canada

0. **Introduction**

Within Canada electronic voting for federal elections is not used, paper ballots are still the primary method of voting for the federal government. Municipalities have the ability to determine their method of voting. This report reviews the experience of 3 Canadian localities with Internet voting systems, and two that may be planning a site test soon.

British Columbia. In February 2014, British Colombia's Independent Panel on Internet Voting published its findings on Internet voting and the related issues of implementation within the province and local government elections (1). The panel discussed the potential and actual benefits of Internet voting, and challenges or difficulties that might ensue. They later filed their recommendations with the Legislative Assembly of British Columbia to not implement universal Internet voting for local government (1).

But the panel commented further: if the system is implemented nonetheless, several steps should be taken to ensure vote security. These steps include but are not limited to limiting Internet voting to individuals with accessibility challenges, coordinate Internet voting by province, and evaluate Internet voting systems with an established technical committee and guidelines proposed within the publication (1).

The guidelines from the British Colombia panel do not meet the definition of end-to-end verifiable. The guidelines lack public verifiability of an election tally and individual votes, so we classify the system in Group 3.

By 2011 the municipalities of Markham, Peterborough, and Halifax have implemented Internet voting (4). These municipalities used their Internet voting systems in conjunction with electronic voting technologies for local election.

The **Halifax** Regional Municipality introduced Internet voting in 2008 as a pilot project (4). The Internet voting system used by the municipality of Halifax was provided by Intelivote. With this system voters were not required to register; instead they could use a PIN number assigned with voter cards and birth dates to authenticate to the system. Voting with this system was restricted to an advanced voting period, in 2009 voting with this system was enabled during the entire voting period (4).

The **Town of Marklam** first offered Internet voting in 2003. With this system voting was possible from the polling place and uncontrolled personal computers during a specific early voting period (4). This system also worked in conjunction with paper based poll voting. Election Systems and Software (ES&S) provided the Internet voting system to the Town of Marklam in 2003 and 2006. In 2010 the service was divided, ES&S providing electronic polling place voting equipment and Intelivote providing the Internet voting system (4). With this system voters received a voter information package which contained a registration PIN and website address for the voting system. With this information the voter would register to vote, access voting system website, authenticate with password and PIN, and make ballot selections (4).

The City of Peterborough introduced Internet voting for municipal elections in 2006. The system used by the City of Peterborough was provided by Dominion Voting Systems. Voters could receive a PIN by either mail or email. This PIN along with additional login information was used to access the voting system.

Both the Halifax Regional Municipality and the Town of Marklam after introducing Internet voting commissioned an *Independent Risk Analysis on Alternative Voting Methods* (4). The findings of the study concluded that polling place voting was the least risky form of voting (4).

The internet voting systems introduced by these 3 municipalities do not meet the guidelines for end-to-end verifiable voting. It is unclear whether there is any method of verifying votes. Thus, we must classify these as Group 3 systems.

On April 28, 2014 the Corporation of the **Municipality of Brockton** proposed an agreement with Dominion Voting Systems to provide Internet Voting services to the municipality. The service the Municipality of Brockton requested includes anonymous votes, audit functionality, recounts, third party review, and fail safe and redundancy (2).

a. Future

The future of Internet Voting in Brockton, Ontario is uncertain. There are Brockton Councilors and citizens that have concerns with Internet voting security and Dominion Voting provisions limiting liability, auditing and recounting, and the lack of opportunity for computer experts to fully test the system (3). Some believe Internet Voting should not be allowed (3).

The **City of Toronto** Council has voted to use Internet voting for individuals with disabilities for the 2014 municipal election (5). This decision was made even with the advice against such actions from subject matter experts.

In conclusion, none of the systems listed above meet the requirements of an end-to-end verifiable voting system and therefore must be classified as Group 3.

Sources

(1) Independent Panel on Internet Voting, British Colombia
(2) Brockton Canada Dominion Voting
(3) http://blackburnnews.com/midwestern-ontario/midwestern-ontario-news/2014/04/15/brockton-councillor-concerned-with-internet-voting-security/
(4) http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf
(5) http://www.toronto.ca/legdocs/mmis/2014/cc/bgrd/backgroundfile-66912.pdf

Estonia

0. Introduction

The nation of Estonia (officially entitled the Republic of Estonia) has been seeking to promote e-government (1). It provides many government services via the Internet and electronic devices to its citizens, including online voting. The Estonian Internet Voting System was launched in 2005 for local government council elections (2). This online voting system does not replace the traditional method of in-person voting at a polling station but constitutes a supplement to it for those who chose it. Traditional voting is given priority over the Internet voting system, meaning traditional voting methods overwrite the votes cast by the Internet voting system. This service is available for use only during 7 days of advance polls (3). The Estonian Voting System has issues with vote integrity and software independence and therefore does not meet the definition of an E2EV system.

1. Core Architecture & Operation

1.1 Basic Architecture & Design

The Estonian Voting System uses the envelope method. Without electronics or the Internet this method involves the voter identifying him/herself, generally with a government identification card, to the polling commission. The voter then receives two envelopes and a ballot. On one envelope they write their credentials. The other envelope is used to hold the filled ballot and is placed within the previous envelope. Once the vote is received by the polling commission the credentials on the outer envelope are verified. They inner envelope (containing the ballot) is then placed in the ballot box. This methodology allows for anonymity and vote privacy. Figure 1 provides a graphic illustration of this process.

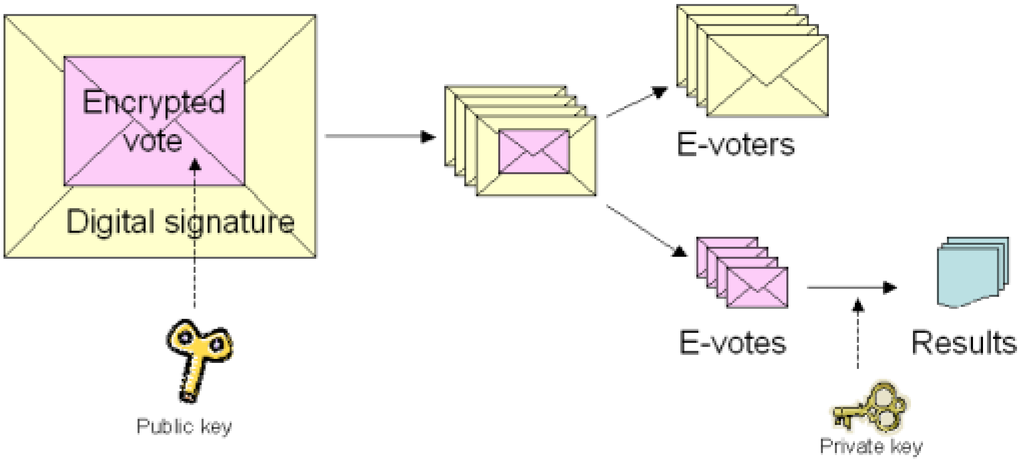


Figure 1 (3)

The Estonian Voting System uses the preexisting public-key infrastructure government issued identification cards as a means of identification and authentication for citizens. Voters have the option of using mobile phones as another form of identification for the voting process as well. The combination of government issued identification card and/or mobile phones, public key infrastructure, and a downloadable I-voting application enables secure voting with the Estonian Voting System. All votes are encrypted prior to transmission over the public Internet via the downloadable I-voting system (3).

1.2 Voting Process

The voting process for the Estonian Voting System first begins with identification which can occur via government issued identification or mobile identification. Mobile identification implements the subscriber identification module (SIM) to identify and authenticate a voter.
If a voter uses and government issued identification card the process is as follows:

1. Voter opens webpage, uses a card reader and government identification card to authenticate.
2. Verifies identify by using personal identification number (PIN1) associated with government identification card.
3. Server checks and verifies credentials of voter.
4. Ballot of appropriate electoral district candidates is displayed to voter.
5. Voter chooses candidate, which is encrypted by the I-voting application.
6. Voter confirms candidate decision by using a PIN2.
7. A confirmation message is displayed to voter and ballot is cast.
8. On the evening of Election Day the encrypted votes and the digital signatures (identity of voter) are separated. The now anonymous electronic votes (e-votes) are opened and counted.

If a voter uses a mobile phone as a form on identification, the voting process is as follows:

1. Voter opens webpage for voting.
2. Voter enters mobile number into website. A control code is then sent to voter’s phone via SMS.
3. Voter identifies themselves by enter the PIN1 into the phone.
4. A ballot associated with their electoral district is displayed on the computer screen.
5. The voter selects their preferred candidate, which is encrypted by the I-voting. A control code is again sent to their phone via SMS.
6. Voter confirms their choice by entering a second PIN (PIN2) in their mobile phone.
7. A confirmation screen is displayed on the computer screen confirming the vote to be cast.

8. On the evening of Election Day the encrypted votes and the digital signatures (identity of voter) are separated. The now anonymous e-votes are opened and counted.

The process of voting with the Estonian Voting System involves a network structure that ensures significant security measures for voters. Below is a diagram of the network system architecture for the Estonian Voting System:

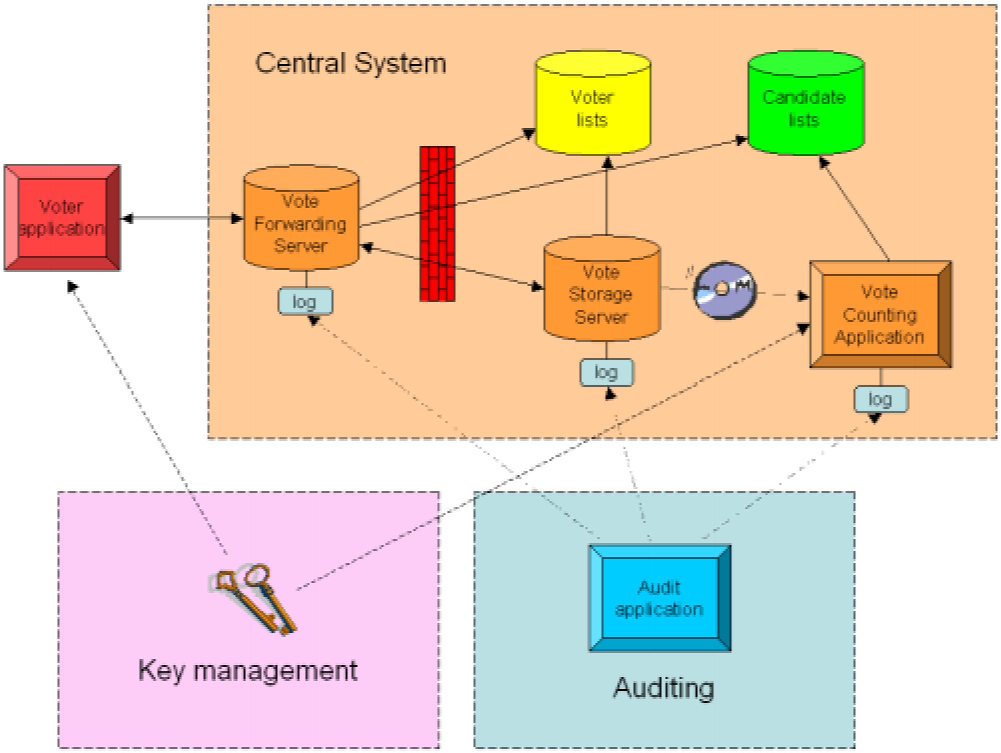


Figure 2 (3)

Each element in the architecture diagram plays a vital role in the operation of the Estonian Voting System.

- Voter Application: The voter's personal computer, which creates the vote via the downloadable I-Voting application, encrypts and digitally signs, and sends the vote to the Central System. The I-voting application is a software application that ensures the security of the voter's device and encrypts the vote prior to being sent to the central system.
- Central System: This system is managed by the National Electoral Committee, and receives and processes votes.
- Key Management: This element of the system generates and manages the key pair(s) for the system. This includes keys for the I-Voting application (public key) and the private keys for the Vote Counting Application.

- Auditing: This element logs all events within the system, allowing for dispute resolution.
- Voter List: This element provides the list of voters and is provided by the Population Register.
- Candidate List: This element provides the list of candidates for ballots and is provided by the National Electoral Committee.
- Vote Forwarding Server (VFS): This element authenticates voter via government issued identification, displays candidates pulled from the candidate list, and receives the encrypted and digitally signed e-Vote. Once the vote is received it is sent to the Voter Storage Server (VSS). A confirmation is sent from the VSS back to the VFS which is then sent to the voter.
- Vote Storage Server (VSS): This element receives and stores votes from the VFS. Upon the closing of advanced polls this element removes double votes, cancels votes from ineligible voters, and processes e-vote cancellation orders. This element also separates e-votes from a voter’s identity (inner envelopes from outer envelopes).
- Vote Counting Application (VCA): This element receives e-votes that have been separated from voter’s identity, tabulates those votes, and outputs the tally of e-votes. This element is kept, segregated offline, from the remainder of the system.

2. Security & Trust

2.1 Security Overview

The security of the Estonian Voting System is unclear. There has been no significant testing of the system by independent certified security experts or guidelines (external to the vendor). With limited knowledge of the resilience of the system configuration, services, and administration little can be said of the systems security. It depends greatly on the security of the Estonian identity card system that is used for voter authentication.

A limited test conducted by Joseph Kiniry brought to light several security issues with the system. This test was conducted with code from the system that was released on July 13, 2013. In this test Joseph Kiniry found several security issues including poor software engineering practice, lack of documentation, lack of vote auditing, and suspicious code borrowing (7). Although the Estonian Voting System appears to offer system for Internet voting, the findings by Joseph Kiniry and lack of vote verifiability prevent the system from be classified as a secure end-to-end verifiable voting system. In short the system not only lacks several key security measures, but also auditability, independent testing, and transparency (5).

2.2 Trust Structure

There are several elements within the Estonian Voting System that require trust on the part of the voter. These elements include the government identification and mobile phone for identification purposes, the computer and web browser for integrity, the integrity of the central system, and finally the local election officials.

2.3 Dispute Resolution

Disputes can be rectified with the logs kept by the Central System. These logs record events occurring within the system. These events include received votes, cancelled votes, cotes to be counted, invalid votes, and accounted votes (3). Although it is possible for voters to verify their vote based upon these logs, that capability is not currently incorporated into the voting system. The voter does not have the ability to verify their vote was recorded and cast correctly by the Central System. Therefore the voter also does not have the ability to dispute erroneous votes.

2.4 Documented Security Issues and Hacks

Threat scenarios that could affect this system include malicious network actors, and malicious LEO. The voting system is vulnerable to server side attacks from possible state actors or grass root malicious actors. Without open-ended vulnerability testing, it is unclear whether the central system is resilient against denial of service attacks and vote-changing malware. Nor can it be established that the online voting system is resilient to sophisticated viruses, or in any given election context has not been compromised. Malicious insider attacks for modifying vote totals is also a possible threat. Without significant auditing and transparency of both administrator activities and any changes to system configurations, a malicious insider could tamper with the votes – yet election officials would likely not discover this intrusion.

2.5 Voter Coercion Resistance

The Estonian Voting System incorporates several security measures to prevent voter coercion. One such measure is allowing voters to vote as many times as they want during a specified pre-voting period (4). This measure prevents coercion because each previous vote is cancelled by the new vote cast by the voter. A second security measure to prevent voter side malware attacks is the downloadable I-Voting application. This measure uses randomization and public key infrastructure to encrypt the vote ensuring its integrity and privacy.

3. Auditability

An Audit application is used to record events within the central system. These events include received votes, cancelled votes, votes to be counted, invalid votes, and accounted votes (3). The auditing application uses hash of a vote and a personal identification code.

4. Vote Privacy

Vote privacy is ensured by the envelope method, the separation of the e-vote from the voter identity upon reaching the central system.

5. **Testing and Deployments**

On July 11, 2013 code was released by the Estonian government. This code was analyzed by Joseph Kiniry and was found to be engineered poorly (7). Several issues such as poor documentation, improper usage of previously published code, lack of validation code, and lack of proper authentication process (7). Lack of validating the code can lead to improper actions by the system that can compromise the confidentiality and integrity of votes.

No other published test and development information is publically available. This system has not undergone other security or performance testing by independent security experts (external to the vendor).

The system is currently in use within Estonia for binding government elections. The Organization for Security and Cooperation in Europe/Office for Democratic Institutions and Human Right (OSCE/ODIHR) observed the March 2011 election with the Estonian Voting System (8). From their report several conclusions were made regarding the security of the system. The OSCE/ODIHR expressed concerns over vulnerabilities pertaining to voters' privacy, voter device malware, insider threat, potentiality for attacks on the central election servers, lack of system transparency, and the lack of a security evaluation of the system by independent computer security experts (5).

6. **Usability and Accessibility Assessments**

There have been no usability and accessibility assessments for this system.

7. **Infrastructure Requirements**

Infrastructure of the Estonian Voting System is based upon government issued identification. System functionality also relies upon the public Internet infrastructure speed and bandwidth and citizen's accessibility to public Internet and Internet enabled devices.

Sources:

(1) http://www.freedomhouse.org/report/freedom-net/2012/estonia
(2) http://estonia.eu/about-estonia/economy-a-it/e-voting.html
(3) http://vvk.ee/voting-methods-in-estonia/engindex/
(4) http://e-estonia.com/component/i-voting/
(5) https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/
(6) http://vvk.ee/public/dok/General_Description_E-Voting_2010.pdf

(7) Joseph Kiniry conference call and PowerPoint presentation

French

0. Introduction:

France was one the earliest country that adopted internet voting. It first experimented with Internet voting in Voisins-le-Bretonneux via a kiosk in 2001. It is better known for its use of remote Internet voting for the election of its Assembly of French Citizens Abroad (AFE). So far, there have been four deployments, the 2003 AFE election for French voter residing in U.S., the 2006 AFE election for French voters residing abroad, the 2009 AFE election for French voters residing in the Americas or Africa, and the 2012 Parliamentary election for all French expatriates.

Scytl, in partnership with Atos Origin, was the technology provider for voting platform in the 2009 and 2012 elections. The voting systems used, however, are close sourced. During the 2012 election, remote Internet voting is offered as a new voting channel in addition to postal and poll-site voting in 774 locations. Over 240,000 votes were cast electronically, representing over 55% of the total votes cast to directly elect 11 members to the French national parliament. [F3]

1. Core Architecture & Operation

1.1 Basic Architecture & Design;

In 2003, a system with double envelopes was used.

In 2006, the electronic roll and the electronic ballot box were stored on two different computers. An applet was downloaded in the voter’s computer. The applet ensured the validity of the vote (preventing over votes, for instance) and encrypted the ballot with the public key. A second validity check was performed on the ballot when it reached the server storing the votes.[F1, p118]

In 2009, the Pnyx system from Scytl was used. Features of this system include:

- “Continuous audit process Opida and Ministry representatives performed random audits of the voting platform components before, during and after the election.
- End-to-end encryption: Votes were encrypted and digitally signed in the voting terminal before they were sent to the voting servers.
- Mixing protocol: Any correlation between voting order and votes was broken using a cryptographic mixing, shuffling and decryption scheme.

- Voter verifiability: Voters can verify the presence of their votes using cryptographic voting receipts that do not disclose voter intent.” [F2, p51]

2. Security & Trust

2.1 Security

Although all the systems are required to abide by the recommendations made by the CNIL (Commission nationale informatique et liberté, or National Commission on IT and Freedom), which provides guidelines for Internet voting systems and updates them over the years, little is known about them beyond the CNIL requirements.[F2,p50]

In June 2006, the Association Démocratique dês Français de l’Étranger – Français du Monde asked François Pellegrini to conduct an evaluation of the Internet voting system in use since 2003, which revealed several security concerns: [F2, p50]

- *“ The secrecy of the vote could be violated due to the small number of people voting over the Internet and the fact that the Chairperson and each Voting Office received a list of the voters (by method) and the total votes cast for each candidate.*
- *The system use third party libraries and the source code were not available if corrections or alterations in the program were necessary.*
- *The hardware was considered proprietary and not available for verification.*
- *Internet voting is subject to results being destroyed or falsified by a small group of individuals in various ways, including: denial of service attacks, DNS (Domain Name System) poisoning or viruses.*
- *The system did not produce hardcopies of data or information.”*

Opida, incorporated security standards from the National Agency of Information

Technology Security (ANSSI), performed security certification of the Scytl voting platform. [FN2,p50]

3. Auditability

The 2006 and 2009 decree mandate that an independent expert audit the confidentiality, security, accuracy and ballot operation control guarantees, before the opening of the ballot. The expert shall have sole access to the source code. He shall hand over his report to the ministry of foreign affairs and to the electoral commission.[F1, p119]

No publication, however, was available to the public.

Group IV Systems

Adder

0. Introduction: Adder Voting System was a concept developed by the University of Connecticut which was founded on "Transparency" and consisted of "Web-based Bulletin board, Token based access control, Privacy and Trust Distribution."[1] The system was suppose to be a e2e-v system that would be universally verifiable, private, and trustworthy

1. Core Architecture & Operation

1.1 Basic Architecture & Design: The adder voting system was setup to be a Internet based voting system that would utilize two web servers, a gatekeeper server, the main server that houses adder, a number of databases, and a token system for the voters. The tokens would be encrypted, and unique, which would allow for the voters to vote anonymously. They also planned on using a bulletin board system for posting the election results and for the voters to verify their votes with their tokens.

2. Security & Trust

"ADDER is an Internet-based e-voting system based on a strong voting-oriented cryptographic primitive (homomorphic encryption)."[2] The system was suggested to have a homomorphic encryption system governing their ballots and votes. Outside of this information, no other data or resources have been mentioned or referred to by the Adder developers. The program was never finished and new information has not be released regarding the security and trust.

3. Auditability

The system suggested a bulletin board for posting results and allowing the general public to verify the votes. There has been no third party testing to prove if these claims are true.

Future

Adder's was first and only released was in 2007. Adder has been on hiatus since 2009.

Reference

- Kiayias, Aggelos, and University of Connecticut. "Adder : Electronic Voting and Decision Making." CryptoDRM Laboratory. University of Connecticut School of Engineering, 14 Aug. 2008. Web. <http://cryptodrm.engr.uconn.edu/adder/>.
- MN, Anusha, and Srinivas BK. "Remote Voting System for Corporate Companies Using Visual Cryptography." Ijarcsse. Ijarcsse, June 2012. Web. <http://www.ijarcsse.com/docs/papers/June2012/Volume_2_issue_6/V2I600261.pdf>.

- Aggelos, Kiayias, Michael Korman, and David Walluck. "An Internet Voting System Supporting User Privacy." CryptoDRM Laboratory. University of Connecticut, 12 Dec. 2006. Web. <http://cryptodrm.engr.uconn.edu/adder/acsac.pdf>.

Horizon Systems

Prêt à Voter: *Horizon, in-person E2EV*

Introduction

Prêt à Voter an in-person voting system was designed in 2004 by Peter Y.A. Ryan from University of Luxembourg with a team of other researchers/scientists. It has since undergone many iterations. Prêt à Voter (***"Ready to Vote")*** is a paper-based system, which requires the voters to vote in-person while in the determined precinct/voting location. This system aims to be an end-to-end verifiable voting system by employing cryptography. Further, it uses cryptography to maintain the integrity of voting process, voter anonymity & privacy, partial resistance towards voter coercion, and auditability.

Prêt à Voter can be used in elections seeking one vote per race as well as in ranked choice voting systems. Prêt à Voter has been implemented in University Systems Competition (VoComp)[PV 6] [PV 8] and thus many variations have been proposed so far. We conduct our analysis of the system PAV 06 [PV 1] based on the publicly available information and published research papers.

1. Core Architecture & Operation

1.1 Basic Architecture & Design

Voters are required to be present at predetermined voting location and are presented with printed ballots on the spot. This scheme employs election officials, who are in charge of maintaining the cryptographic signatures which are used for printing the encrypted ballots.

Prêt à Voter was written in Java code. By contrast to its earlier version PAV 05 [PV 2] which used the RSA cryptography scheme, version PAV 06 employs the ElGamal cryptographic approach along with re-encryption mixes. Having the ballots encrypted allows the voters to audit the ballots prior to voting and also presents the voters with a coded receipt at the end of voting, which the voters can use to verify their cast ballot vote choices. That the receipts are encrypted helps in achieving voter privacy and resiliency from voter coercion. The cast vote and the results are displayed on an electronic bulletin board, which helps the system to be universally verifiable.

1.2 Voting Process

<u>Printing Ballots</u>: Before ballots are printed, the election officials are required to generate cryptographic keys. A sample ballot is shown in Fig 1. The two values on the bottom of the ballots are the results of the encryption process followed by the election official. These two values hold the cryptographic relation of every row on left hand side (LHS) of the ballot to every row on the right hand side (RHS) of the ballot. The left hand side is used to print the election candidate's names using the bottom LHS code and the right hand side of the ballot is where the voter marks an ' X ' against his choice of the candidate. The bottom RHS value is used to audit the ballot and also used to verify the recorded vote from the bulletin board. Instead of a single election official generating the keys, a number of officials are required to generate the keys, encrypting the candidate order and finally generate the bottom values. It is ensured that every ballot will have a random order of the candidate names.

1fd34fg	Fd333ff

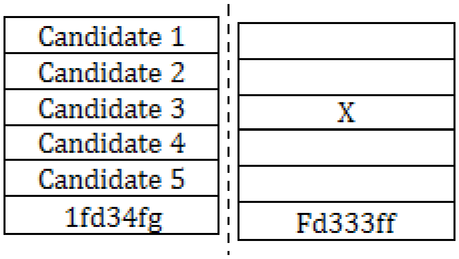
Fig. 1 Sample Ballot

Ballot casting: The voter is provided with a ballot which is printed in his presence. The voter then needs to scan the left hand side of the ballot in the system available, which scans the LHS bottom value and prints the names of the candidates in the left column. This printed ballot is shown in Fig 2. This ballot has a perforation which separates the left side from the right side.

Candidate 1	
Candidate 2	
Candidate 3	
Candidate 4	
Candidate 5	
1fd34fg	Fd333ff

Fig. 2 Ballots with names of candidates

After this step, the voter will mark an ' X ' in the right column corresponding to this choice of candidate. After a selection is made, the voter is required tear of the perforation thus separating the left side from the right side of the ballot as shown in Fig 3



Candidate 1
Candidate 2
Candidate 3
Candidate 4
Candidate 5
1fd34fg

X
Fd333ff

Fig. 3 Vote Codes entered – 6055 & 2392

The left hand side of the ballot is then required to be discarded (for eg by using a paper shredder available) and the right hand side is then again scanned in the system to record the vote. Upon scanning the right hand side, this receipt is shown on a public bulletin board. Voters can compare their receipts with the one shown on bulletin board to confirm that their vote was recorded accurately. A video about the voting process can be found at - http://www.pretavoter.com/index.php

Results: Once all the votes are recorded and displayed to the voters, the election officials are required to perform re-encryption mixing, decryption and tallying (which will include all the votes recorded) [PV 3]. Once this is done the results are shown on the bulletin board.

2. Security Features

This system aims to be an end to end verifiable voting system by employing cryptography and thereby seeks to maintain integrity of voting process, voter anonymity & privacy, receipt freeness, resiliency towards voter coercion(partially) and ability to be auditable. The earlier proposed version PAV 05 [PV 2] used RSA scheme, while PAV 06 employs ElGamal scheme along with re-encryption mixes.

3. Voter Privacy & Coercion resistance

Since the candidate names are randomized on the left hand side and while ballot casting the left hand side is destroyed, it ensures that no one can trace which voter voted for which candidate. Also since the final receipt only has a 'X' mark with a random value, this does not reveal which candidate did the voter vote for. Moreover, since the ballots are printed on demand, this ensures that no blank ballot can be taken out of the voting place; thus saving from Chain attack. This attack is described in [PV 1] as follows "The attack works as follows: the coercer smuggles a blank ballot form out of the polling station. The controls on the distribution of the forms should make this a little tricky, but in practice there are many ways it could be achieved. Having marked the form for the candidate of their choice, the coercer intercepts a voter as they enter the polling station. The voter is told that if, when they exit the polling station, they hand a fresh, blank form back to the coercer they will receive a reward. The attack can now proceed inductively until a voter decides to cry foul".

4. Integrity and Auditability

All the stages of the Prêt à Voter voting system (ballot casting, ballot recording & tallying) are completely auditable. Ballots can be audited by the voters before casting their ballot as well as any changes/discrepancies in the ballot recording can be detected by the voter. Also the tally phase can be audited by an auditor. All the stages provide enough trails which enable to detect any compromise to the integrity of the voting process. Additional schemes such as Human readable paper audit trail [PV 4] and using Voter verified paper audit trail have been suggested to further enhance the auditability of the system.

5. Infrastructure required

By the election official –

4. Officials who will generate the master secrets for generating the codes
5. Hardware for printing the ballots
6. Hardware for scanning the ballots and discarding the left hand side of ballots

By the voter –

3. A computer with internet connection to verify the results on Bulletin Board

Shortcomings

We have seen so far that Prêt à Voter is a paper-based in-person voting system that is an end-to-end verifiable system. This means that it is capable of ensuring the integrity of the votes, results, and privacy of the voters. Additionally, it is partially resilient to coercion. However, this system is susceptible to another form of coercion: Randomization attack[34]. Even though no single election official can generate a key or decrypt the votes, if the relevant officials collude, there is a possibility that integrity may be compromised without being detected. The system can also be compromised inadvertently through weak key management practices.

This system is not capable of operating when faced with a DOS attack. We also did not have any data on the usability aspects of this voting system. A newer version of this system is being proposed for the absentee voter in a remote setting [PV 1]. At this point, it is premature to comment on any aspects of the remote version, other than to watch for its release and later evaluations.

References:

[PV 1] Prêt à Voter with re-encryption mixes, Peter Y.A. Ryan, S.A. Schneider. - http://epubs.surrey.ac.uk/7219/2/esorics06.pdf

[PV 2] A Practical, Voter-Verifiable Election Scheme, David Chaum, Peter Y.A. Ryan et al - http://www.cs.ncl.ac.uk/publications/trs/papers/880.pdf

[PV 3] The Prêt à Voter Verifiable Election System, Peter Y.A. Ryan et al - http://www.pretavoter.com/publications/PretaVoter2010.pdf

[PV 4] Human readable paper verification of Prêt à Voter, David Lundin & Peter Y.A. Ryan . - http://epubs.surrey.ac.uk/2804/1/LUNDIN_human_readable_paper.pdf

[PV 5] A Case Study in System-Based Analysis: The Three Ballot Voting System and Prêt à Voter, Peter Y.A. Ryan et. al. - http://www.nowires.org/Papers-PDF/casestudy.pdf

[PV 6] Experiences Gained from the first Prêt à Voter Implementation, Peter Y.A. Ryan et. al - http://epubs.surrey.ac.uk/7211/2/revote09.pdf

[PV 7] http://www.pretavoter.com/

[34] Randomization attack is defined as: "Adversaries can coerce voters to bring out their receipts with the choice marks always at the top. Although they do not know how these voters have cast their votes, they make these voters vote in a random manner" [PV 3]

[PV 8] http://www.vocomp.org/index.php.html

Civitas – Horizon -Remote E2E System

Introduction

Civitas is a remote voting system designed by Michael R. Clarkson, Stephen Chong and Andrew C. Myers from Cornell University. This system is presented in the paper published in May 2007 called "Civitas: Toward a Secure Voting System" [C 1]. This being a remote voting system proposes to achieve integrity by providing verifiability as well as resistance to coercion. Our analysis is based on the publicly available literature and interviews with the individual architects and/or developers.

1. Core Architecture & Operation

1.1 Basic Architecture & Design

Civitas is designed in JIF language [C 2] and Java. It uses cryptographic schemes such as Diffie-Hellman, RSA, ElGamal and employs zero knowledge proofs, while in the experimentation done by the above team the system used 128-bit AES keys, 2048-bit RSA keys, and 224-bit ElGamal keys. Civitas is implemented using the JCJ scheme (Juels, Catalano, and Jakobson [C 3] with some enhancements as discussed in [C 1]. Fig. 1 below shows the Civitas architecture and the basic flow of the voting process, taken from [C 1].

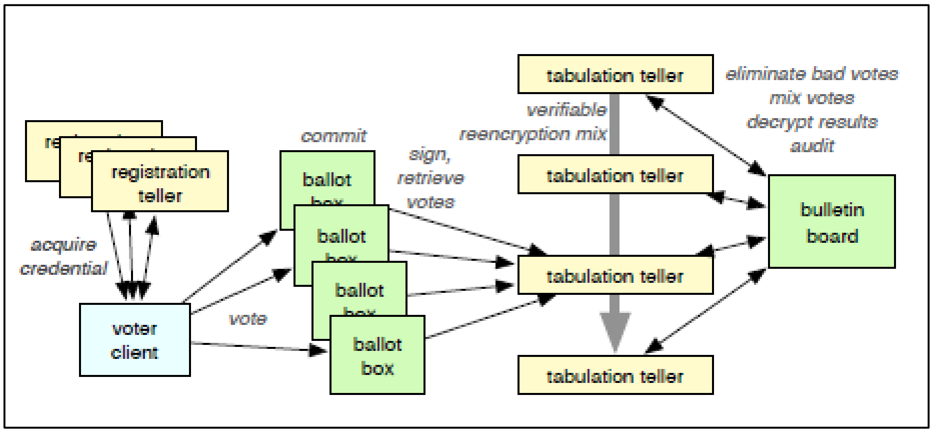


Fig. 1

It is important to note that for remote voting Civitas does not distinguish between postal voting and internet voting. The proposed features of Civitas would ultimately rely on how this system is adopted and deployed in a real election.

1.2 Voting Process

The Civitas system proposes the following: In this system, the voters can be registered online or in person with an election official (depending if the online channel is compromised). The election officials are required to generate certain public and private key pairs which are required during the election. This would mean that the actual deployment of Civitas system would require use of a Public Key Infrastructure.

All the public keys (for election officials and voters) along with the election roll (which can contain either the voter names or their registration numbers) and the ballot design are posted on the publicly accessible bulletin board.

Unique voter credentials are generated which are used to authenticate voters while preserving voter anonymity. The voters are provided with two secrets called the 'registration key' and the 'designation key'. The voters are registered using their registration key. Then as described in [C 1] "The teller and voter then run a protocol, using the voter's designation key, which releases the teller's share of the voter's private credential to the voter. The voter combines all of these shares to construct a private credential." "To vote, the voter submits a private credential and a choice of a candidate (both encrypted), along with a proof that the vote is well-formed, to some or all of the ballot boxes[35]."

After this, as part of the tally process; all the votes are taken from the ballot box and verified for their well-formedness cryptographically, then anonymized using mix nets (after removing duplicate entries). After anonymizing, it is made sure that unauthorized votes (from unauthorized credentials – discussed below is section #4) are removed and then the results are displayed on the bulletin board. The final results are publicly verifiable and voters can check if their vote was added in the final tally (this can be done using zero-knowledge proofs). It is important to note that all the entries on the bulletin board are insert-only and are digitally signed and all the stages of the voting process are auditable.

2. Security Features

As mentioned earlier, Civitas was written in JIF and Java. JIF is "a security-typed programming language that extends Java with support for information flow control and access control, enforced at both compile time and run time" [C 2]. This system proposes to achieve integrity by providing verifiability. This system also proposes to be auditable at all the stages of the voting process as well as it proposes strong voter coercion resistance.

2.1 Trust Structure

Following are some of the trust assumptions required for its security features to hold true:

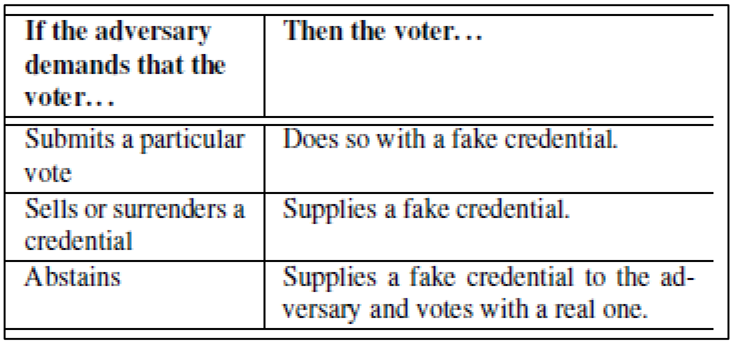
1. Voters need to trust at least one election official
2. Voters need to trust the device/client used by them
3. Voters need to trust the link between them and the election official, during registration
4. The channel used to cast the vote should be anonymous
5. Voters need to trust at least one ballot box

[35] A server/system with a database is called a ballot box, which is able to record all the incoming votes.

More details can be found in [C 1]

4. Coercion Resistance

For achieving Coercion resistance, voters are provided with the capability to generate fake credential (either online or in person; depending on how the system is deployed). These fake secret credentials are generated using cryptographic protocols and the voter's designation key (note – this process does not change the voter's public credentials). Thus, to a coercer these fake credentials will be indistinguishable from the real credentials. Fig.2 below highlights scenarios for coercion and the corresponding action required by the voter (source [C 1]):



If the adversary demands that the voter...	**Then the voter...**
Submits a particular vote	Does so with a fake credential.
Sells or surrenders a credential	Supplies a fake credential.
Abstains	Supplies a fake credential to the adversary and votes with a real one.

Fig. 2

5. Integrity and Verifiability

The system proposes to maintain integrity by prescribing universally verifiable protocols (as described in voting process). Since the results are displayed on a publicly accessible bulletin board, voters can verify if their choices have been recorded accurately and their vote has been counted in the tally. Any changes can be detected by the voters as well as election officials. Also, since all entries are digitally signed and are insert-only, it improves upon the property of integrity.

Shortcomings

We have seen that this system proposed features include strong coercion resistance, verifiability, and integrity. This system was not designed for availability, however the literature proposes this can be achieved by additional features. Moreover, even though no single election official can generate a key or decrypt the votes, there is a possibility that integrity may be compromised if the officials collude. It remains to be seen, how this system will be adopted and deployed in a real election; as aspects related to security features, usability, availability will rely on how well the final implementation is.

References:

[C 1] Civitas: Toward a Secure Voting System, Michael R. Clarkson, Stephen Chong, Andrew C. Myers, Cornell University, May 2007 https://www.cs.cornell.edu/projects/civitas/papers/clarkson_civitas_tr.pdf

[C 2] JIF: Java Information Flow- http://www.cs.cornell.edu/jif/

[C 3] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In Proc. of Workshop on Privacy in the Electronic Society, pages 61–70, Nov. 2005. http://markus-jakobsson.com/papers/jakobsson-wpes05.pdf

[C 4] *Civitas.* Virginia Tech NCR, September 14, 2012 http://faculty.cs.gwu.edu/~clarkson/talks/clarkson_civitas_vtncr.pptx

Comparative Metrics for Group 1 Systems

Metrics Compilation – Group 1 Systems

CATEGORY	FACTORS	REMOTEGRITY	HELIOS	RIES - NETHERLAND
User Trust	1. Whom or what does the voter need to trust that			
	1.1. An authentic blank ballot from LEO is delivered to the voter's computer/device. Must voter trust			
	a) Voter's own computer/device?[36]	No	Yes	No
	b) The Internet and the ISPs -- of voter's internet service & election office?[37]	No	Yes	No
	c) Local election officials?	Yes	No	No
	d) Computer equipment or software at the LEO, such as a server, network, +/or the VS software	No	Yes	Yes
	e) Some third party, such as a printing company or other vendor, e.g., for delivery of printed or the creation of coded electronic ballots, which are accurately mapped to the candidates' names?	Yes	Yes	Yes
	1.2. Voter's ballot contains the choices that voter had marked at the time he/she attempts to return the marked/voted ballot to the LEO, specifically that no change has occurred between the voter's marking the ballot & the LEO's receipt of the marked ballot. Must voter trust			
	a) Voter's own computer/device? [38]	No	Yes	Yes
	b) The Internet and the ISPs -- of voter's internet service & election office?	No	Yes	Yes
	c) The Internet (for transmission of the voted ballot)?	No	Yes	Yes

[36] In other words, can malware on the voter's computer change the voter's ballot such that the voter cannot detect changes (an inauthentic ballot) & these are changes are also undetectable at the election office?

[37] For instance, does the voting system send authentic ballots that are not susceptible to change by personnel or automated malware at the ISP or at other intermediate internet transmittal "hops"?

[38] In other words, could malware change the voter's ballot choices such that the changes are undetectable at the election office? This might occur in some systems if malware on the voter's computer can covertly modify the vote choices before the ballot is transmitted to the LEO. If the voter must independently check—i.e., "audit" the ballot that the LEO has received

	d) The local election officials personally?	No	No	No
	e) Computer equipment at the LEO, such as a server, network, +/or the VS software.	No	Yes	Yes
	f) A vendor that administers the election for LEO/outsourcing	No	Unclear	Unclear
	1.3. Voter's marked ballot is correctly recorded in the tabulation database at election office - Must voter trust-			
	a) Voter's own computer/device? [39]	No	No	Yes
	b) The Internet and the ISPs -- of voter's internet service & election office?	No	No	Yes
	c) The Internet (for transmission of the voted ballot)?	No	Yes	Yes
	d) The local election officials personally?	No	No	Yes
	e) Computer equipment at the LEO, such as a server, network, +/or the VS software.	No	Yes	Yes
	f) A vendor that administers the election for LEO/outsourcing	No	Unclear	Unclear
	g) VS electronic "Bulletin Board"	No	Yes	No
Voter Anonymity	1. Is it possible to associate or connect the identity of a voter with a particular cast ballot or vote, at the point of			
	a. Voter's transmittal of a marked ballot to the election office, over the internet?	No	Unclear	Yes
	b. At LEO, the recording of vote choices in the database?	No	No	No
	c. Reporting of final results?	No	Yes	No
Security	*1. Was the system tested for security vulnerabilities by security experts?* Were:	Yes	No	Yes
	1.1. ***Network security vulnerabilities*** identified?	Unclear	Unclear [40]	Unclear
	a) If yes, how many vulnerabilities?	Unclear	Unclear	Unclear
	b) Were the vulnerabilities fixed?	Unclear	Unclear	Unclear

[39] In other words, could malware change the voter's ballot choices such that the changes are undetectable at the election office? This might occur in some systems if malware on the voter's computer can covertly modify the vote choices before the ballot is transmitted to the LEO. If the voter must independently check—i.e., "audit" the ballot that the LEO has received.

[40] Due to the lack of security testing for the Helios System by a reliable third party, the ability to establish the existence or lack of existence of any vulnerabilities has been compromised. In light of these developments, all scenarios that may address any vulnerabilities have been labelled as "unclear" until testing has occurred.

	c) If not, are they planned to be fixed?	Unclear	Unclear	Unclear
	d) Have the vulnerability fixes been independently reviewed by qualified security experts?	Unclear	Unclear	Unclear
	1.2. ***Application security vulnerabilities*** identified?	Yes	Unclear	Unclear
	a) If yes, how many vulnerabilities?	Unclear	Unclear	Unclear
	b) Were the vulnerabilities fixed?	Yes	Unclear	Unclear
	c) If not are they planned to be fixed?	N/A	Unclear	Unclear
	d) Have the vulnerability fixes been certified by security experts?	Unclear	Unclear	Unclear
	2. Were the results of such testing published internally or publically?	Unclear	Unclear	Yes
	3. Is the system resilient to:			
	a. Client side malware?	Yes	No	No
	b. Server side malware?	Yes	No	Unclear
	4. Does the system allow detecting changes to the integrity of the votes during:			
	a. Casting of ballots?	Yes	Yes	Yes
	b. Recording of casted ballots?	Yes	Yes	Yes
	c. Tallying the recorded ballots?	Yes	Yes	Yes
	5. Can the changes to integrity detected, be corrected in the system?	Yes	Unclear	Yes
	5.1. Is the recovery process Automated or manual?	Manual	Unclear	Automated and Manual
	6. Is there a defined Recovery Time Objective[41] associated with the system?	Unclear	Unclear	Unclear
	7. Is there a defined Recovery Point Objective[42] associated with the system?	Unclear	Unclear	Unclear
	8. Does the voting system incorporate any technical or administrative measure to deter, prevent, detect, and defend against Voter Coercion?	No	No	No
	9. Does the voting system incorporate any technical or administrative measure to deter, prevent, detect, and defend against LEO coercion?	No	No	Unclear

[41] The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity

[42] Recovery point objective is the maximum tolerable period in which data might be lost from an IT service due to a major incident

Auditability	1. Does the system produce a voter-verifiable, durable, tamper-evident artifact (abbreviated "V V-D-TEA")?[43]	Yes	No	Yes
	2. Can any additions, deletions, or substitutions to the voter's ballot selections (votes) be detected, using the V V-D-TEA records?	Yes	No	No
	3. Can the results of the election contests (races and issues) be reconstructed (recounted) independently of using the voting system's software, simply by using the V V-D-TEA records?[44]	Yes	Yes	No
	4. Does the system require additional audit checks, for instance by using digital signatures and hashes?	Yes	Yes	Yes
	5. Does the voting system support the auditing of:			
	a) Number of blank ballots sent to voters	Yes	No	Yes
	b) Number of voted ballots received from voters	Yes	Yes	Yes
	c) Verifiability of cast as recorded	Yes	Yes	Unclear
	d) Verifiability of tallied as cast	Yes	Yes	Yes
	6. Does the auditability design of the voting system require via hard-coded [nondiscretionary, within range of reasonability] logs of operators' interaction with:			
	a) Blank ballots generator/database	Yes	Unclear	Yes
	b) Voted ballots collection system/database	Yes	Unclear	Yes
	c) Cast ballots storing system/database	Yes	Unclear	Unclear
	d) Cast ballots tallies	Yes	Unclear	Unclear
	e) Cast ballots reports	Yes	Unclear	Unclear
	f) System failures, malfunctions and other threats or attacks on operation of the voting system, as well as other infrastructure components	Yes	Unclear	Yes
	7. Are these audit logs protected from administrative or operator modifications (insider threat)?	Yes	Yes	Unclear
	8. Are these audit logs protected against operations (e.g., system crashes) or attacks which could lead to data corruption or loss?	Yes	Yes	Unclear
	9. Does the audit system maintain voter anonymity at all times?	Yes	Yes	No

[43] Noted voting system auditing expert Dr. Phillip Stark recommended this set of attributes that we have abbreviated "V V-D-TEA."

[44] This question asks for whether the system can be described as producing a voting record and potential for election results that are "software independent." See Rivest & Stark, and Stark & Wagner (cites)

Testing & Development	1. Has the system received reliability testing or any other testing specified by the Voluntary Voting System Guidelines (VVSG)?	No	No	Unclear
	2. Has the system been submitted for certification under the EAC voting system process?	No	No	No
	3. Has the system received open-ended vulnerability testing, as recommended by the EAC's Technical Guidelines Development Committee?	No	No	Unclear
	4. Has the system undergone any other independent testing, not by the internal developers but by a qualified independent organization or set of individuals?	No	No	Yes
	5. Have the developers announced any planned independent testing?	No	No	No
	6. Is the system currently or planned to be deployed for:			
	a) Public Government election?	No	No	Yes
	b) Private, nonprofit, labor union election?	No	Yes	No
Usability	1. Has a usability study been conducted by qualified usability assessors and published for public or scholarly access?	No	Yes	Yes
	2. If yes, did the study report deficiencies in the system with regard to usability by voters, specifically regarding			
	a) Comprehension & success in ***marking*** of ballot?	Unclear	Yes	Unclear
	b) Comprehension & success in ***casting*** of ballot?	Unclear	Yes	Unclear
	c) Comprehension & success in ***verifying*** of ballot?	Unclear	Yes	Unclear
	3. Did the study report usability deficiencies in the system with regard to election official set up of the election?	Unclear	No	Unclear
Accessibility	1. Has an accessibility study been conducted by qualified accessibility assessors, published by public or scholarly access?	No	No	Unclear
	2. Is the system designed for persons with physical impairments that may affect voting?			
	a) Blind	Unclear	No	No
	b) Deaf	Unclear	Yes	No
	c) Multiple impairments	Unclear	Unclear	No

Score Assignment

(High – 5, Medium – 3, Low – 0)

Area	Score Assignment to responses
User Trust	No = 5, Yes = 3, Unclear =0
Voter Anonymity	Yes = 5, No = 0, Unclear =0
Security	Yes = 5, No = 0, Unclear = 0
Auditability	Yes = 5, No =0, Unclear = 0
Testing & Development	Yes = 5, No =0, Unclear = 0
Usability	Yes = 5, No =0, Unclear = 0
Accessibility	Yes = 5, No =0, Unclear = 0

Systems Score Table

Area	Max Possible Score	Remotegrity	Helios	RIES
User Trust	90	86	58	58
Voter Anonymity	15	15	5	10
Security	110	50	15	30
Auditability	85	85	40	40
Testing & Development	35	0	5	10
Usability	25	0	20	5
Accessibility	20	5	5	0

Bibliography

Adder

1. [AD1]Kiayias, Aggelos, and University of Connecticut. "Adder : Electronic Voting and Decision Making." CryptoDRM Laboratory. University of Connecticut School of Engineering, 14 Aug. 2008. Web. <http://cryptodrm.engr.uconn.edu/adder/>.
2. [AD2]MN, Anusha, and Srinivas BK. "Remote Voting System for Corporate Companies Using Visual Cryptography." Ijarcsse. Ijarcsse, June 2012. Web. <http://www.ijarcsse.com/docs/papers/June2012/Volume_2_issue_6/V2I600261.pdf>
3. [AD3]Aggelos, Kiayias, Michael Korman, and David Walluck. "An Internet Voting System Supporting User Privacy." CryptoDRM Laboratory. University of Connecticut, 12 Dec.

Arizona

1. http://www4.nau.edu/srl/PressReleases/99f%20-%20Internet%20Voting.pdf
2. http://www.wired.com/2009/06/cfp-evote/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+wired27b+(Wired%253A+Blog+-+Threat+Level)

Canadian System

1. Independent Panel on Internet Voting, British Colombia
2. Brockton Canada Dominion Voting
3. http://blackburnnews.com/midwestern-ontario/midwestern-ontario-news/2014/04/15/brockton-councillor-concerned-with-internet-voting-security/
4. http://labs.carleton.ca/canadaeurope/wp-content/uploads/sites/9/AComparativeAssessmentofInternetVotingFINALFeb19-a.pdf
5. http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

Civitas

1. [C 1] Civitas: Toward a Secure Voting System, Michael R. Clarkson, Stephen Chong, Andrew C. Myers, Cornell University, May 2007 https://www.cs.cornell.edu/projects/civitas/papers/clarkson_civitas_tr.pdf
2. [C 2] JIF: Java Information Flow- http://www.cs.cornell.edu/jif/
3. [C 3] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In Proc. of Workshop on Privacy in the Electronic Society, pages 61–70, Nov. 2005. http://markus-jakobsson.com/papers/jakobsson-wpes05.pdf
4. [C 4] Civitas. Virginia Tech NCR, September 14, 2012 http://faculty.cs.gwu.edu/~clarkson/talks/clarkson_civitas_vtncr.pptx

Democracy Live

1. "ELECTRONIC BALLOTING." Democracy Live Inc. N.p., n.d. Web. 17 Apr. 2014. <http://democracylive.com/>.

Estonia

1. http://www.freedomhouse.org/report/freedom-net/2012/estonia
2. http://estonia.eu/about-estonia/economy-a-it/e-voting.html
3. http://vvk.ee/voting-methods-in-estonia/engindex/
4. http://e-estonia.com/component/i-voting/
5. https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/
6. http://vvk.ee/public/dok/General_Description_E-Voting_2010.pdf
7. Joseph Kiniry conference call and PowerPoint presentation

Everyone Counts

1. [E1C1] “Introduction to eLect system”, Everyone Counts, http://www.everyonecounts.com/introduction-to-elect/
2. [E1C2, p6] “Request for Information: Uniform Voting System for the State of Colorado”, Everyone Counts Inc. April 1, 2013
3. [E1C 3] “Submission to the Inquiry into the future of Victoria’s electoral administration”, Everyone Counts, Feb 1, 2013
4. [E1C 4] “Problems with the iVote Internet Voting System”, Venessa Teague and Roland Wen, 2011
5. [E1C 5] “Increasing Accessibility to Voting with New Technology”, An Everyone Counts White Paper, September 2012
6. [E1C 6] “Submission to the Inquiry into the 2012 Local Government Elections”, Everyone Counts, Aug. 2, 2013

French System

1. [F1] “International Experience with E-Voting”, Jordi Barrat i Esteve, Ben Goldsmith and John Turner, Norwegian E-Vote Project, June 2012
2. [F2] “Testing and Certification Technical Paper #2: A survey of Internet Voting”, U.S. Election Assistance Commission, September 14 2011
3. [F3] "French Expats Vote Online in Legislative Elections with Scytl's Technology" . Scytl. June 25 2012.

Helios

1. Adida, Ben. "Helios: Web-based Open-Audit Voting." USENIX Security (2008): n. pag. Web. <static.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf>.
2. Adida, Ben. "Helios: A Deeper Look." Telephone interview. Transcript.
3. Karayumak, Fatih, Maina M. Olembo, Michaela Kauer, and Melanie Volkamer. "Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System." CASED:Technische Universit ̈at Darmstadt (n.d.): n. pag. Web. <http://www.usenix.org/event/evtwote11/tech/final_files/Karayumak7-27-11.pdf>.
4. Weber, Janna-Lynn, and Urs Hengartner. "Usability Study of the Open Audit Voting System Helios." JannaWeber.com. Janna-Lynn Weber, Sept. 2009. Web. <http://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf>.
5. University of Washington, Orion. "Security Review: Helios Online Voting." UW Computer Security Research and Course Blog. University of Washington, 13 Mar. 2009. Web. <https://cubist.cs.washington.edu/Security/2009/03/13/security-review-helios-online-voting/>.
6. SecVote, Dagsthul. "Usable Verifiable Remote Electronic Voting Case Study HELIOS." SecVote. SecVote, 18 July 2012. Web. <http://secvote2010.uni.lu/slides/mvolkamer-usability.pdf>.

IOASIS

1. GSN. "South Dakota Secretary of State Activates IOASIS Computerized Military Voting System." Government Security News. GSN, 28 Mar. 2014. Web. 16 Apr. 2014. <http://www.gsnmagazine.com/article/40653/south_dakota_secretary_state_activates_ioasis_comp>.
2. Plyler, Kim. "IOASIS to Streamline Voting Process for Overseas Personnel." Scoop. Scoop World, 27 Mar. 2014. Web. 16 Apr. 2014. <http://www.scoop.co.nz/stories/WO1403/S00335/ioasis-to-streamline-voting-process-for-overseas-personnel.htm>.

Los Angeles

1. Los Angeles. "Voter & Election Information." Voter & Election Information. Los Angeles, n.d. Web. 15 Apr. 2014. <http://www.lavote.net/Voter/>.
2. Los Angeles. "Inkavote Plus." Voter & Election Information. Los Angeles, n.d. Web. 15 Apr. 2014. <http://www.lavote.net/Voter/Inkavote_Plus.cfm>.

Maryland

1. Maryland. "Overview of Maryland's Voting System." Voting System Overview. Maryland, n.d. Web. <http://www.elections.state.md.us/voting_system/index.html>.
2. Kazanjian, Glynis. "MarylandReporter.com." Maryland Prepares Move Back to Paper Ballots for Elections. Maryland Reporter, 19 Nov. 2013. Web. <http://marylandreporter.com/2013/11/19/maryland-prepares-move-back-to-paper-ballots-for-elections/>.
3. Jefferson, David, and Candice Hoke. Risks Presented by On-Screen and Online Electronic Ballot Marking. Security Review. N.p.: n.p., n.d. Print.
4. Kazanjian, Glynis. "Online Ballot Tool Goes Uncertified over IT Security Concerns." Local News ATOM. Cumberland Time News, 28 Apr. 2014. Web. 01 May 2014. <http://www.times-news.com/local/x493481867/Online-ballot-tool-goes-uncertified-over-IT-security-concerns>.

Norway

1. [NC1] “Can we trust internet voting? Internet voting in Norway”,Henrik Nore,The Ministry of Local Government and modernization, ONPE-OAS Lima, October 21 2013.
2. [NC2] “The Norwegian Internet Voting Protocol”, Kristian Gjosteen, Department of Mathematical Sciences, Norwegian University of Science and Technology, August 9, 2013
3. [NC3] “Technical report Source code audit of Norwegian electronic voting system Ministry of Local Government and Regional Development”, Tor E. Bjørstad, *mnemonic*, August 07 2013
4. [NC4] “Norway Parliamentary Elections 9 September 2013, Osce/Odihr Election Assessment Mission Final Report”, Office for Democratic Institutions and Human Rights, December 16 2013
5. [NC5] “Compliance with International Standards”, Jordi Barrat i Esteve and Ben Goldsmith, Norwegian E-Vote Project, June 2012
6. [NC6] Notes taken from Joe Kiniry’s presentation on “Reflections on Internet Voting Internationally”, April 17 2014
7. [NC7] “Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting”, Oliver Spycher, Melanie Volkamer and Reto Koenig, *E-Voting and Identity, Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, pp 19-35*

Pret a voter

1. [PV 1] Prêt à Voter with re-encryption mixes, Peter Y.A. Ryan, S.A. Schneider. - http://epubs.surrey.ac.uk/7219/2/esorics06.pdf
2. [PV 2] A Practical, Voter-Verifiable Election Scheme, David Chaum, Peter Y.A. Ryan et al - http://www.cs.ncl.ac.uk/publications/trs/papers/880.pdf
3. [PV 3] The Prêt à Voter Verifiable Election System, Peter Y.A. Ryan et al - http://www.pretavoter.com/publications/PretaVoter2010.pdf
4. [PV 4] Human readable paper verification of Prêt à Voter, David Lundin & Peter Y.A. Ryan . - http://epubs.surrey.ac.uk/2804/1/LUNDIN_human_readable_paper.pdf
5. [PV 5] A Case Study in System-Based Analysis: The Three Ballot Voting System and Prêt à Voter, Peter Y.A. Ryan et. al. - http://www.nowires.org/Papers-PDF/casestudy.pdf

6. [PV 6] Experiences Gained from the first Prêt à Voter Implementation, Peter Y.A. Ryan et. al - http://epubs.surrey.ac.uk/7211/2/revote09.pdf
7. [PV 7] http://www.pretavoter.com/
8. [PV 8] http://www.vocomp.org/index.php.html

Remotegrity

1. [R1] Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System, Filip Zagorski et.al. - https://eprint.iacr.org/2013/214.pdf
2. [R2] A. Essex, J. Clark, U. Hengartner, and C. Adams. Eperio: Mitigating technical complexity in cryptographic election verification. - https://eprint.iacr.org/2012/178.pdf
3. [R3] Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy, David Chaum et.al. - https://www.usenix.org/legacy/events/sec10/tech/full_papers/Carback.pdf
4. [R4] Remotegrity FAQ - http://www.scantegrity.org/wiki/index.php/Remotegrity_Frequently_Asked_Questions#What_can_go_wrong_with_Remotegrity.2C_and_how_will_you_protect_against_it.3F
5. [R5] Cryptographic Voting Debuts, MITnews, http://web.mit.edu/newsoffice/2009/rivest-voting.html
6. [R6] Remotegrity Poster - http://zagorski.im.pwr.wroc.pl/papers/Remotegrity-poster.pdf
7. [R7] Takoma Park Public Bulleting Board - http://takoma.remotegrity.org/BulletinBoardFinal.php
8. [R8] B. Adida. Helios: web-based open-audit voting. In USENIX Security Symposium- static.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf

RIES

1. [RN1] “RIES - Internet Voting in Action”, Engelbert Hubbers, Bart Jacobs and Wolter Pieters, *Security of Systems, Nijmegen Institute for Computing and Information Sciences*, Radboud University Nijmegen

2. [RN2]" RIES - Rijnland Internet Election System:A Cursory Study of Published Source Code", Rop Gonggrijp, Willem-Jan Hengeveld, Eelco Hotting, Sebastian Schmidt, and Frederik Weidemann , *E-Voting and Identity, Second International Conference, VOTE-ID 2009, Luxembourg, September 7-8, 2009*, pp 157-171
3. [RN3] "Description and Analysis of the RIES Internet Voting System", Engelbert Hubbers, Bart Jacobs Berry Schoenmakers Henk van Tilborg Benne de Weger, *Institute for the Protection of Systems and Information (EiPSI),Faculty of Mathematics and Computer Science Eindhoven University of Technology*, version 1.0, June 24, 2008
4. [RN4] Query results from Competence Center for Electronic Voting and Participation, http://db.evoting.cc/index.php?page=database&sub=query_quick, last accessed April 9 2014
5. [RN5] Compliance of RIES to the Proposed e-Voting Protection Profile, Hugo Jonker, Melanie Volkame, *E-Voting and Identity-First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007,* pp 50-61
6. [RN6] Electronic elections employing DES smartcards. Herman Robers. Master's thesis, Delft University of Technology, December 1998.
7. [RN7]"Rijnland Internet Election System (RIES) facts and features sheet", Pont Piet Maclaine, *Workshop on UOCAVA Remote Voting Systems – Position Papers*, *2010*, version 2.0,July 28th 2010

Scantegrity

1. (1) http://www.scantegrity.org/papers/ScantegrityII-EVT.pdf
2. (2)https://www.usenix.org/legacy/events/evt08/tech/full_papers/chaum/chaum_html/index.html
3. (3) http://www.scantegrity.org/wiki/index.php/Software_Design_Document

Scytl

1. [SCY1]Software Review and Security Analysis of Scytl Remote Voting Software, Michael Clarkson, Brian Hay, Meador Inge abhi shelat, David Wagner, Alec Yasinsac, September 19, 2008

2. [SCY2] http://kleinonline.wnd.com/2012/10/26/confirmed-spanish-firm-to-provide-overseas-military-ballots-absentee-voter-requests-currently-down-by-staggering-numbers/
3. [SCY3] Attacking the Washington, D.C. Internet Voting System, Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012
4. [SCY4] http://www.cbc.ca/news/politics/ndp-site-the-weak-link-in-online-attack-during-2012-leadership-vote-1.2557861
5. [SCY5] http://digitalvote.wordpress.com/tag/electronic-voting-pilot-test-scytl/
6. [SCY6] http://www.scytl.com/news/scytl-security-protocols-ensure-clients-unaffected-heartbleed-bug/
7. [SCY7] http://www.scytl.com/e-election-platform/
8. [SCY8] Voter self verification, Scytl, http://www.scytl.com/products/election-day/scytl-online-voting/

Star-Vote

1. [ST 1] STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System, USENIX JETS vol. 1, #1, August 2013, Josh Benaloh et. al. - https://www.usenix.org/system/files/conference/evtwote13/jets-0101-bell.pdf
2. [S2] STAR Vote- http://www.traviscountyclerk.org/eclerk/content/images/presentations_articles/cuc_presentation/pdf_tc_elections_5b_CUC_presentation_life_of_ballot.pdf
3. [ST 3] Election Verifiability or Ballot Privacy: DoWe Need to Choose? Cryptology ePrint Archive, Report 2013/216. (2013), Edouard Cuvelier et al. - https://eprint.iacr.org/2013/216.pdf
4. [ST 4] 2013 EVT/WOTE presentation by Dan Wallach - https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell

E2E-V

1. LAWRENCE NORDEN, PROJECT DIRECTOR. THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST. Tech. New York: Brennan Center for Justice, 2006. Print.
2. Stark, P.B., and D.A. Wagner. "Evidence-Based Elections." Evidence-Based Elections. IEEE Security and Policy, 14 Jan. 2012. Web. 01 May 2014.
3. Wolchok, Scott, Eric Wustrow, Dawn Isabel, and Alex J. Halderman. "Attacking the Washington, D.C. Internet Voting System." Attacking the Washington, D.C. Internet Voting System. In Proc.16th Conference on Financial Cryptography & Data Security, Feb. 2012. Web. 01 May 2014.
4. Hoke, Candice. "Internet Voting: Structural Governance Principles for Election Cyber Security in Democratic Nations." Internet Voting. Cleveland State University, 2009. Web. 01 May 2014.
5. Jefferson, David. "Why Voting Transactions Are Different from Financial Transactions." Why Voting Transactions Are Different from Financial Transactions. Electionlawblog, 11 Nov. 2011. Web. 01 May 2014.
6. Jefferson, David, Aviel D. Rubin, Barbara Simons, and David Wagner. "Analyzing the Security of Internet Voting." VOTING SECURITY. University of California, Berklee, 20 Jan. 2004. Web. 01 May 2014.
7. Joaquim, Rui, Paulo Ferreira, and Carlos Ribeiro. "EVIV: An End-to-end Verifiable Internet Voting System." Science Direct. N.p., 2 June 2012. Web. 01 May 2014.
8. Popoveniuc, Stefan, John Kelsey, Andrew Regenscheid, and Poorvi Vora. "Performance Requirements for End-to-End Verifiable Elections." Usenix.org. Usenix.org, 9 Aug. 2010. Web. 01 May 2014.
9. Simons, Barbara, and Douglas Jones. "Internet Voting in the U.S." Communications of the ACM. ACM.org, 12 Oct. 2012. Web. <http%3A%2F%2Fcacm.acm.org%2Fmagazines%2F2012%2F10%2F155536-internet-voting-in-the-us%2Ffulltext>.
10. Gallagher, Sean. "Iranians Hacked Navy Network for Four Months? Not a Surprise." Ars Technica. Ars Technica, 19 Feb. 2014. Web. 01 May 2014. <http://arstechnica.com/information-technology/2014/02/iranians-hacked-navy-network-for-4-months-not-a-surprise/>.