Diaspora Online Voting

Presented by: Department of CSE, BUET

Outline of This Presentation

- Diaspora voting – from the vault
  - Expert opinions
  - Case Studies
  - Expected features

- Our proposal based on expected features
  - Registration process
  - Internet Oblivious (IO) voting

we Create
we Simulate
we Emulate...

Summary of Resources We Looked over

Voting from Abroad

The International IDEA Handbook

INTERNATIONAL IDEA INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

Out-of-Country Voting: A Brief Overview

Peter Erben, Ben Goldsmith, Aysha Shujaat

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS IFES 25 YEARS

GEO-ECONOMICS AND POLITICS

What is e-voting? Who's using it and is it safe?

Apr 4, 2024

WORLD ECONOMIC FORUM

UNIVERSITY OF MINNESOTA Human Rights Library

ElectionGuard: a Cryptographic Toolkit to Enable Verifiable Elections

Josh Benaloh and Michael Naehrig, *Microsoft Research;* Olivier Pereira, *Microsoft Research and UCLouvain;* Dan S. Wallach, *Rice University*

https://www.usenix.org/conference/usenixsecurity24/presentation/benaloh

Articles

How did Estonia carry out the world's first mostly online national elections

Post date: March 7, 2023

Security Analysis of the Estonian Internet Voting System

Drew Springall[†] Travis Finkenauer[†] Zakir Durumeric[†]
Jason Kitcat[‡] Harri Hursti Margaret MacAlpine J. Alex Halderman[†]
[†]University of Michigan, Ann Arbor, MI, U.S.A.
[‡]Open Rights Group, U.K.

electronic voting

Ask the Chatbot a Question | More Actions

Written by René Peralta
Fact-checked by The Editors of Encyclopaedia Britannica
Last Updated: Mar 3, 2025 • Article History

Britannica

ELECTIONS

Voting online is very risky. But hundreds of thousands of people are already doing it

UPDATED SEPTEMBER 8, 2023 · 1:13 PM ET

Miles Parks

npr

Working Group Statement on Developing Standards for Internet Ballot Return

CENTER FOR SECURITY IN POLITICS
UNIVERSITY OF CALIFORNIA, BERKELEY

Berkeley Public Policy The Goldman School

CENTER FOR THE STUDY OF SECURITY IN POLITICS

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

HAL open science

MEXICO TO IMPLEMENT ELECTRONIC VOTING FOR GENERAL ELECTIONS

Written by EVoting Communications / 04 de Enero del 2024

Mexico: Transforming Electoral Participation

Successful Implementation of Internet Voting for Mexicans Abroad

we Create
we Simulate
we Emulate...

Ways of Voting from Abroad

- Personal voting
- Postal voting
- Proxy voting
- Electronic means
  - Use Internet, PDAs, phones, etc., to cast vote
  - Most often referred to as remote electronic voting or e-voting
- Other methods: Vote by fax (Australia and New Zealand)

INTERNATIONAL IDEA INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

Ways of Voting from Abroad – From A Different Lens

- Return Voting
- In-Person Polling Station
- Embassy Voting
- Postal Voting
- Internet Voting

Fundamentals of Diaspora Voting

- “the <u>basic operational and electoral rules and regulations</u> have to be followed so that the short cuts do not endanger the overall security and accountability of the electoral process.”
    - "Voting from Abroad” by The International IDEA Handbook

Fundamentals of Voting

- Security, transparency, secrecy, accuracy, integrity, swiftness, privacy, auditability, accessibility, cost-effectiveness, scalability, ecological sustainability, fault tolerance, accessibility, non-repudiation, etc.

- Security
  - Identity and freeness
- Transparency
  - Possibility of recounting
- Secrecy
  - Anonymity

- "Voting from Abroad" by The International IDEA Handbook

Voting – As Per Human Rights

- “The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret ballot or by equivalent free voting procedures."
    - The Universal Declaration of Human Rights, Article 21

Requirements in Internet Voting

- End-to-End Verifiability (E2E-VIV)
  - Cast as intended
  - Recorded as cast
  - Tallied as recorded
- Security
- Usability
- Transparency

Internet/E- Voting

- (+) Helps voters living in remote areas or abroad
- (-) Include risks of cyber-attacks or software errors
- (-) Identifying and verifying online votes can also be difficult
- (-) Vulnerable to penetration by various types of malware
- (-) Possibility of voter coercion and vote selling

- Can be planned in small scale

A Case Study - TIVI (Trust, Innovation, Verifiability, Integrity)

- The Instituto Nacional Electoral (INE) (Spanish for National Electoral Institute) of Mexico engaged Smartmatic
- In 2024 general elections, Mexico, citizens residing abroad to vote online
    - ~70% voted online
- Voting from any electronic device (tablet, mobile phone, or computer)
- Access to an electronic ballot that voters can navigate to cast their votes
- Both remote Internet voting and in-person voting at selected embassies
- Vote verification using a receipt (QR code) sent via SMS or email

MEXICO TO IMPLEMENT ELECTRONIC VOTING FOR GENERAL ELECTIONS

Written by EVoting Communications / 04 de Enero del 2024

A Case Study - TIVI (contd.)

- Advantages
  - Diaspora inclusion
  - Flexibility
  - Verification using QR codes
  - Security using end-to-end encryption and digital signatures
  - Accessibility from various devices
- Disadvantages
  - Limited scope
  - Verification concerns in complete end-to-end verification
  - Digital access barriers
  - Trust issues
  - Proprietary solution

we Create
we Simulate
we Emulate...

A Case Study - ElectionGuard

- Used in actual public U.S. elections in Wisconsin, California, Idaho, Utah, and Maryland
    - Also used for civic voting in the Paris suburb and an online election by a Switzerland/Denmark-based organization
- Separation of the cryptographic tools from the core mechanics and user interfaces of voting systems
    - This separation allows the cryptography to be designed and built by security experts without having to re-invent and replace the existing infrastructure
- Uses ElGamal encryption

ElectionGuard: a Cryptographic Toolkit to Enable Verifiable Elections

Josh Benaloh and Michael Naehrig, *Microsoft Research;* Olivier Pereira, *Microsoft Research and UCLouvain;* Dan S. Wallach, *Rice University*

https://www.usenix.org/conference/usenixsecurity24/presentation/benaloh

A Case Study - ElectionGuard (contd.)

- Advantages
  - Open source
  - Verification without compromising privacy
  - Integration potential
  - Statistical security
  - Multi-stakeholder verification
- Disadvantages
  - Compromised stakeholders
  - Limited implementation
  - Not a complete solution
  - Technical complexity
  - Implementation challenges
  - Client-side vulnerabilities

we Create
we Simulate
we Emulate...

A Case Study - i-Voting

- Estonia - the first nation to hold general elections over the internet in 2005
    - 2023 parliamentary elections - 51% votes were cast online
- Voting is available during an early voting period (several days before Election Day)
- Voters can change their electronic votes unlimited times during this period
- Voters can override their electronic vote by voting at a polling station
- Votes are encrypted and stored with the voter's digital signature
    - On election day, digital signatures are removed to anonymize votes before tallying

Articles

How did Estonia carry out the world's first mostly online national elections

Post date: March 7, 2023

Security Analysis of the Estonian Internet Voting System

Drew Springall† Travis Finkenauer† Zakir Durumeric†
Jason Kitcat‡ Harri Hursti Margaret MacAlpine J. Alex Halderman†

†University of Michigan, Ann Arbor, MI, U.S.A.
‡Open Rights Group, U.K.

A Case Study - TIVI (contd.)

- Advantages
  - Convenience
  - Increased participation
  - Transparency
  - Voter confidence
  - Cost efficiency
- Disadvantages
  - Security concerns
  - Trust prerequisites
  - Digital divide
  - Verification limitations
  - Political controversy

Internet/E- Voting - Researchers' View (contd.)

- A systematic market study and review on academic literature
  - A total of 82 candidate systems
    - 29 Internet voting systems are both in active use and claim to employ some form of verifiability
      - Only 8 systems are well-documented, of which only a few employ state-of-the-art mechanisms
  - Fundamental steps: Cast (Encryption), Authentication, Cast Verification, User and System Record, and Tally

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

https://hal.archives-ouvertes.fr
HAL open science

Expected Features in Our Internet Voting

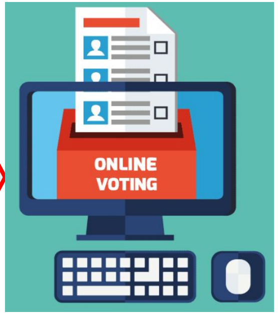
- Cast (Encryption)
  - Asymmetric
  - Distributed Key storage
- Authentication
  - Centralized
  - Directly-entered
  - Cryptographically-bound
- Cast Verification
  - Both audit and cast
- User and System Record
  - Storage and hash
  - Access to individual entry and all entries
  - Centralized consistency

Our Proposal - Internet Oblivious (IO) Voting

Registration through Biometric (image) check and setting secret Qs (several days prior to voting)

Online voting system (with DR)

Login and vote through own registered account (liveliness check and secret Qs)



RSA encryption; Securely saves voting info and BEC nonce - should be decrypted only in case of checking auditability

e-ballot with the selected Voter nonce, and sign of the vote mark

Confirmation by the Voter (with liveliness check and secret Qs)

Separate storage of in BEC -
1. BEC nonce, Hash(BEC nonce, Voter nonce, mark), and mark
2. NID, IP, and timestamp

Online system in BD (BEC)

Second online system (Hot DR of BEC in abroad)

Voter copy with Voter nonce, Hash, and mark (optional) (for auditability, if needed)

Realizes the notion of *oblivious transfer*

Important Steps and Feature in IO Voting

- Registration
- Login
- Random number generation
- Request to vote
- Confirmation
- Storage for future check

- Cast (Encryption)
  - Asymmetric
  - Distributed Key storage
- Authentication
  - Centralized
  - Directly-entered
  - Cryptographically-bound
- Cast Verification
  - Both audit and cast
- User and System Record
  - Storage and hash
  - Access to individual entry and all entries
  - Centralized consistency

Important Considerations in IO Voting

- Precalculation of mapping - (BEC nonce, Voter nonce)
  - In front of representatives of stakeholders
  - Saved in a safe custody with the representatives
- Authentication while login and casting
  - Image, liveliness, and secret Qs
  - # of secret Qs - depends on image and liveliness check
- Verification and system records
  - Voter verification of own voting through hashes
  - Auditing of each vote under tallying through hashes
  - Publisizing the NIDs of diaspora voters for open verification
- Selection of nonce by a voter - stored only at the voter
  - Realizes the notion of Oblivious correspondence

Tentative Roadmap with Timeline

Serial	Task	Duration (months)
1	Design Verification	2-3
2	Onboarding development and R&D sources	0.5-1
3	Requirement analysis, development, and R&D	2-3
4	Different types of testing and R&D	0.5-1
5	User acceptance analysis and piloting	0.5-1
6	Implementation of the first phase	-
	Total	**~6**

Tentative Countries in First Phase

Country	Count	Country	Count
Saudi Arabia	4875000	Cruesia	4000
UAE	1200000	Herzegovina	1000
Oman	800000	UK	1300000
Kuwait	265000	Itali	250000
Qatar	350000	Greece	29078
Bahrain	155587	Belgium	5000
Jordan	70000	Switzerland	4500
Iraq	70000	USA	1282500
Turkiye	3000	Canada	100000
Maldives	100000	Brazil	2500
Brunai	19772	South Africa	250000
Malaysia	1500000	Libia	21000
Singapore	140000	Mouritius	10000
Indonesia	450	Eswatini	2000
Japan	31536	Botswana	1000
China	15000	Gambia	400
South Korea	31220	Namibia	100
Spain	60000	Moozambique	5000
Germani	40000	Lesotho	400
France	100000	Egypt	12000
Netherlands	10000	Australia	129600

Source: BEC

- Considerations
  - Small enough for not exhibiting any substantial risk over the national election
  - Large enough for conducting a meaningful exploration
  - Availability of standard technology preparedness
  - Global diversity

Disclaimers and Way Ahead

- Traditional limitations of the Internet voting remain
- Sufficient brainstorming
  - Comprehensive security audit
  - Critical analysis on corner cases and adversarial models
- Confidence building and public engagement
  - All types of stakeholders - political parties, voters, journalists, technical experts, etc.
- Legal and regulatory framework
- Phased implementation with piloting
  - Can be started from a place whose risk on overall result is low
- Need time (~3 months) for necessary explorations and design validations to confirm conformity with state-of-the-art solutions

Thank You!

(Acknowledgement: Web sources)

Backup Slides

we Create
we Simulate
we Emulate...

Ways of Voting from Abroad - Countries

Procedures	# of cases	Countries
Personal voting only	54	Afghanistan, Angola, Argentina, Azerbaijan, Belarus, Botswana, Brazil, Bulgaria, Cape Verde, Central African Republic, Colombia, Côte d'Ivoire, Croatia, Czech Republic, Djibouti, Dominican Republic, Ecuador, Equatorial Guinea, Finland, Georgia, Ghana, Guinea-Bissau, Guyana, Honduras, Hungary, Iceland, Iran, Iraq, Israel, Kazakhstan, Kyrgyzstan, Laos, Moldova, Mozambique, Namibia, Niger, Peru, Pitcairn Islands, Poland, Romania, Russia, Rwanda, São Tomé and Principe, Senegal, Singapore, South Africa, Sudan, Syria, Tunisia, Turkey, Ukraine, Uzbekistan, Venezuela, Yemen
Postal voting only	25	Austria, Bangladesh, Bosnia and Herzegovina, Canada, Denmark, Falkland Islands, Fiji, Germany, Gibraltar, Guernsey, Ireland, Italy, Jersey, Lesotho, Liechtenstein, Luxembourg, Malaysia, Isle of Man, Marshall Islands, Mexico, Norway, Panama, Switzerland, Tajikistan, Zimbabwe
Proxy voting only	4	Mauritius, Nauru, Togo, Vanuatu
Mixed procedures	27	Algeria, Australia, Belgium, Benin, Chad, Cook Islands, Estonia, France, Gabon, Guinea, India, Indonesia, Japan, Latvia, Lithuania, Mali, Micronesia, Netherlands, New Zealand, Palau, Philippines, Portugal, Slovenia, Spain, Sweden, Thailand, United Kingdom
Not yet implemented or not available	4	Bolivia, Greece, Nicaragua, Oman
Total	**114**	

Note: The United States is not included in this table since the procedures for external voting vary by state

A Comparative View

Procedure	Security	Recounting	Anonymity	Remark
Personal voting	High	Ensured	Ensured	*Difficult to manage*
Postal voting	Medium	Ensured	*Difficult to ensure*	
Proxy voting	*Low*	Ensured	*Not ensured*	
Internet/e- voting	Medium	*Difficult to ensure together*		
Return Voting	High	Ensured	Ensured	*Difficult to manage*

Challenges in Postal Voting

- Registration process
  - Time restrictions
- Timely sending
  - Postal sending needs time
- Availing postal sending services
  - May not be available everywhere

Challenges in Proxy Voting

- Ensuring secrecy
  - Vote gets exposed to another
- Checking liveness
  - Is the voter live during voting?
- Confirming freeness and trust
  - Is the casted vote reflect the intent of the actual voter?
  - Increased possibility of voter coercion and vote selling

- Reargument - used for visually-impaired people
  - Count of visually-impaired people is significantly low
  - Are our non-resident voters like visually-impaired people?

Challenges in Internet/E- Voting

- Recounting
- System reliability
- Networking issues
- Security
- Availing electronic devices for voting

Internet/E- Voting - Researchers' View (contd.)

- Cast (Encryption)

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Encryption																		
symmetric										●								●
asymmetric	●	●	●	●	●	●	●	●				●		●		●	●	
Keys																		
distr. storage	●	●	●	●	●	●	●	●				●		●		●	●	
distr. generation	●	●	●	●		●	●	●										

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

Internet/E- Voting - Researchers' View (contd.)

- Authentication

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Credential Generation																		
centralized	•					•		•				•						
distributed		•																
on the voter's device		•								•	•							•
election-independent					•													
Credential Interface																		
directly entered	•	•				•		•				•						
trusted hardware					•													
Credential Properties																		
cryptographically bound	•	•			•	•		•		•		•						•
distributed authentication		•																

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

Internet/E- Voting - Researchers' View (contd.)

- Cast Verification

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
audit-or-cast		●	●	●			●											
cast-then-audit					●	●						●						●
return codes								●										
clear-text receipts													●		●			
audit codes						●			●				●		●			

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

we Create
we Simulate
we Emulate…

Internet/E- Voting - Researchers' View (contd.)

- User Record

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
User Artifact																		
storage ref		●							●	●	●	●		●	●			●
ballot hash	●		●	●	●	●	●										●	
plain vote													●					
return code								●										
Artifact Properties																		
signed		●			●	●			●								●	
chained										●	●				●			●

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

HAL open science

Internet/E- Voting - Researchers' View (contd.)

- System Record

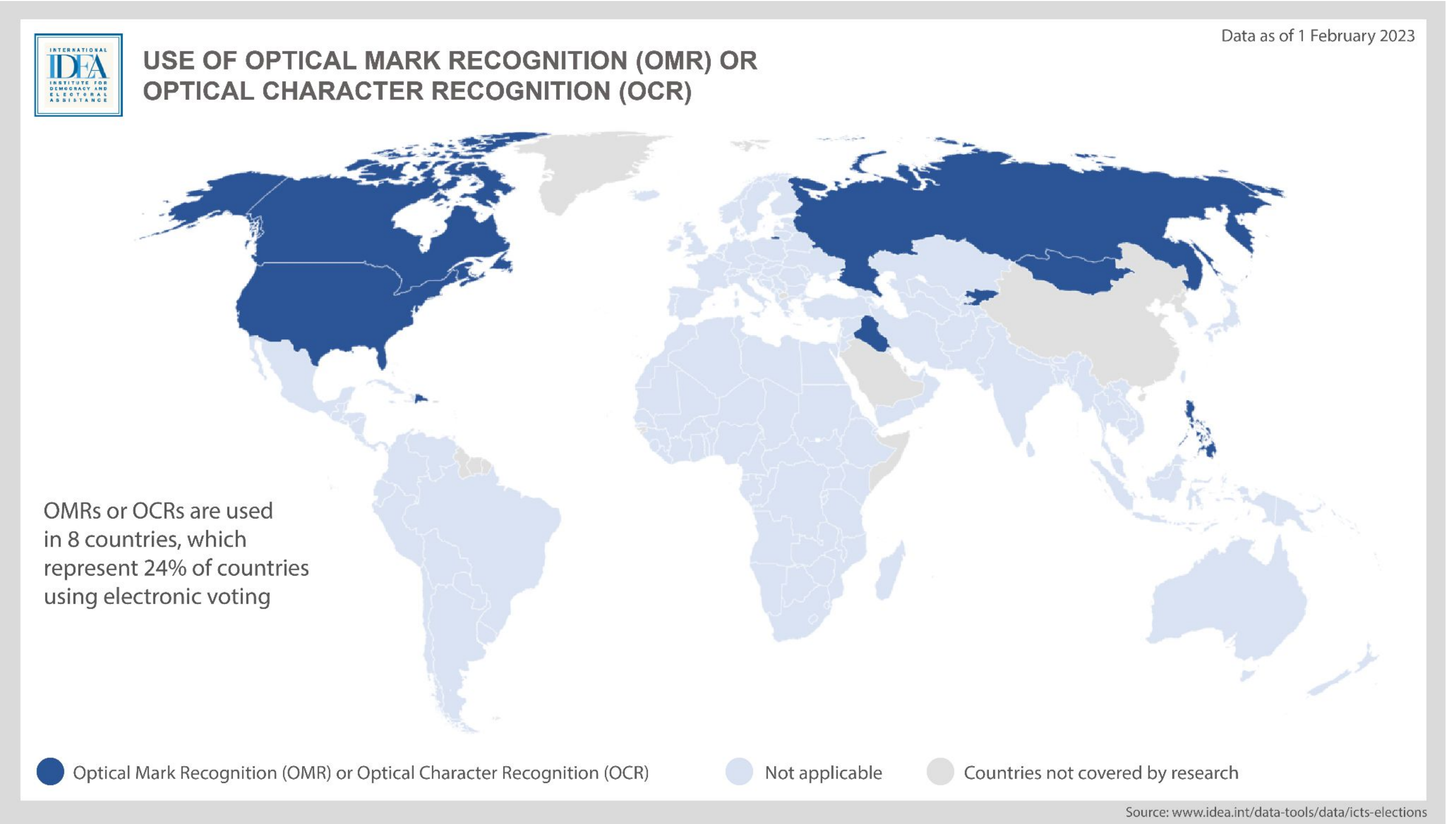
	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Access																		
indiv. entries	●	●	●		●		●		●	●	●	◐	●					●
all entries	●	●	●				●		●	●	●	◐	●	●				●
Consistency																		
centralized	●	●	●	●		●	●											
immediate										●	●				●			●
delayed					●			●										

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

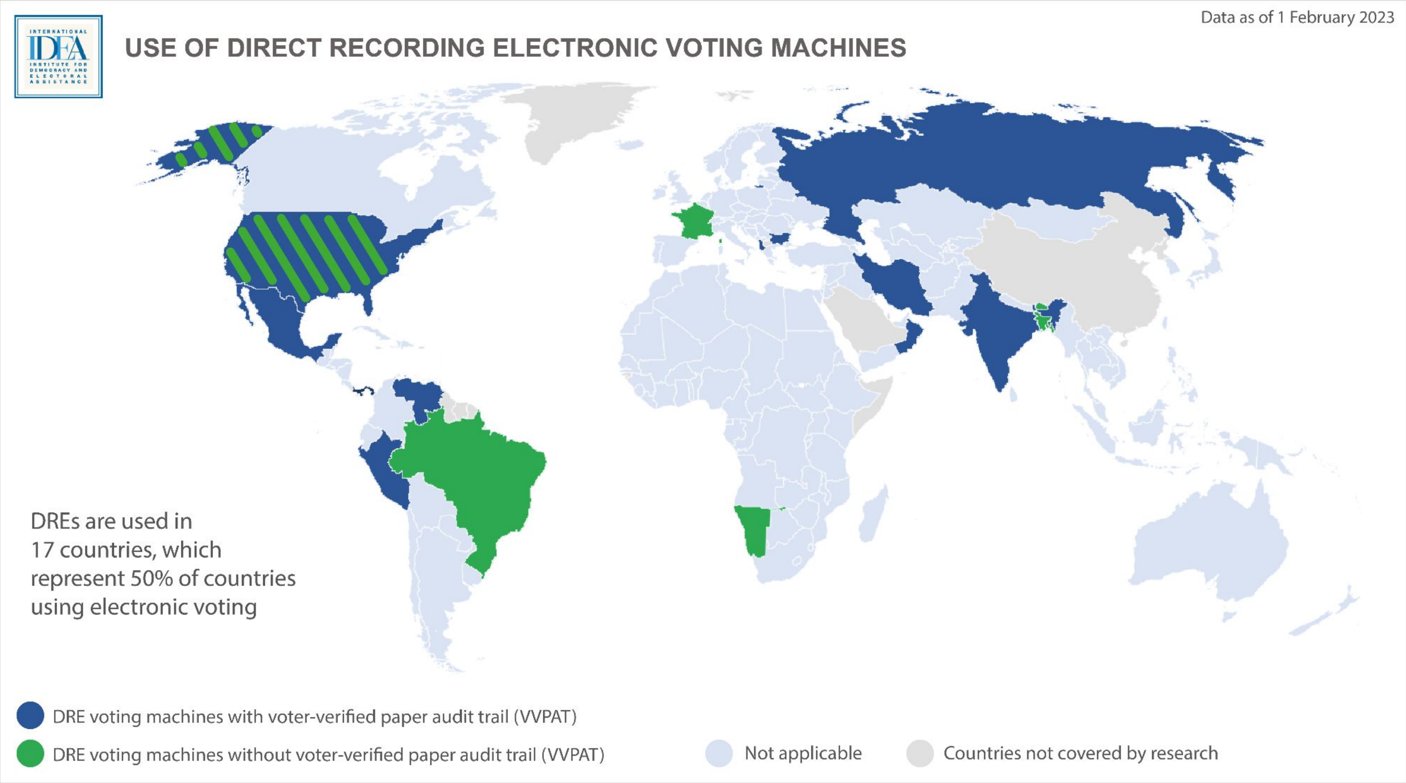
Florian Moser, Michael Kirsten, Felix Dörre

HAL open science

Use of Internet Voting around the Globe



Use of DRE around the Globe



Source: www.idea.int/data-tools/data/icts-elections

Summary of Challenges

- Registration process
- Ensuring security and freeness
- Enabling recounting
- Confirming anonymity
- Timely sending

Our Proposals

- Option 1: In-person E-voting (IE Voting)
    - More acceptable
    - Needs acceptability in the host territories
- Option 2: Internet Oblivious voting (IO Voting)
    - Completely on cyberspace
    - Applicable to all territories

Option 1: In-Person E-Voting (IE Voting)

Biometric check

Embassy or a suitable place

Touch over voted mark

Online system in BD (BEC)

Second online system (abroad)

Printed ballot with a hash (timestamp, mark) and sign of the vote mark

Could be under video surveillance or monitoring of party representatives

***Only* applicable to the places where we have an Embassy or a suitable place, and permission to do so**

we Create
we Simulate
we Emulate…

What to Do if We do NOT have an Embassy or So?

- In-person voting is not a reality
- We must face a trade-off
  - Postal or Proxy or Electronic Voting
    - All should depend on Internet nowadays
      - Registration purposes or so
    - So, why not we have the voting completely on Internet?
      - Trade-off gets limited only to the electronic systems

we Create
we Simulate
we Emulate...

Internet/E- Voting

- (+) Helps voters living in remote areas or abroad
- (-) Include risks of cyber-attacks or software errors
- (-) Identifying and verifying online votes can also be difficult

- Estonia pioneered online voting in 2005, but e-voting systems around the world are still developing

WORLD ECONOMIC FORUM

Internet/E- Voting

- (-) Use of the Internet has been at times massively disrupted by denial-of-service attacks in Estonia
- (-) Vulnerable to penetration by various types of malware
- (-) Possibility of voter coercion and vote selling
- 2 major types of e-voting equipment
  - Direct Recording Electronic (DRE) machines
    - A paper audit record is must
  - Optical scanning machines

Britannica

Internet/E- Voting - Researchers' View

- (-) "The advice from cybersecurity experts is clear: Widespread internet voting at this point is a bad idea"
- (-) "Informally, putting a server online to support online ballot return is like asking a kid to go play in traffic. It just isn't safe"
  - Ron Rivest, a cybersecurity expert who founded the companies RSA and Verisign

Internet/E- Voting - Researchers' View (contd.)

- (-) "Basically every election security expert agrees that we should not have lots of people voting over the internet,"
  - William Adler (senior elections technologist, Center for Democracy and Technology)
- "In most transactions, the results of a failure are traceable and often obvious to all parties involved in a transaction: a bank account balance is wrong, a car is delivered in an unexpected color, a tax burden does not match expectations,"

  "The intentional lack of traceability of a cast ballot back to a voter due to the requirement of a secret ballot demands different technical controls than other types of online transactions."

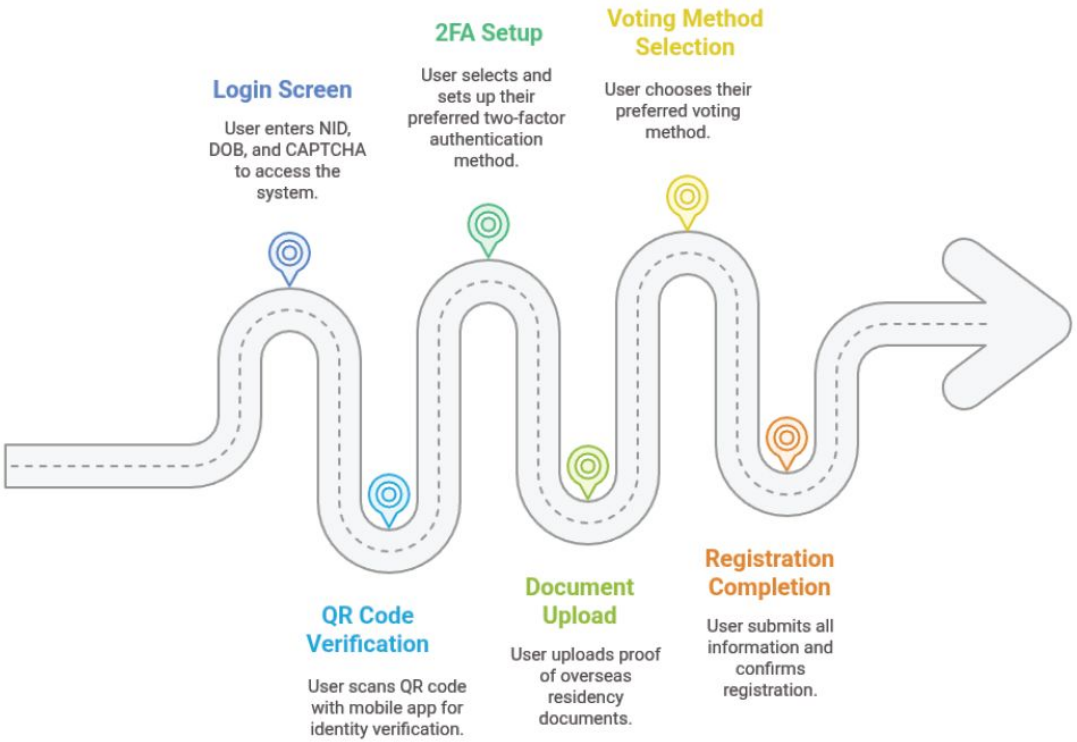
npr

Berkeley Public Policy The Goldman School

A Case Study - ElectionGuard (contd.)

- Encryption of individual votes with a unique identifier
- Voter tracking codes that allow voters to verify their votes counted correctly
- Homomorphic encryption
  - Allows tallying encrypted votes without decrypting individual ballots
- Public verification mechanisms that allow anyone to confirm vote tallies
- Open-source design that enables independent security review
  - Developed by Microsoft

Our Proposal - Registration



Our Proposal - Registration Verification