Final Project

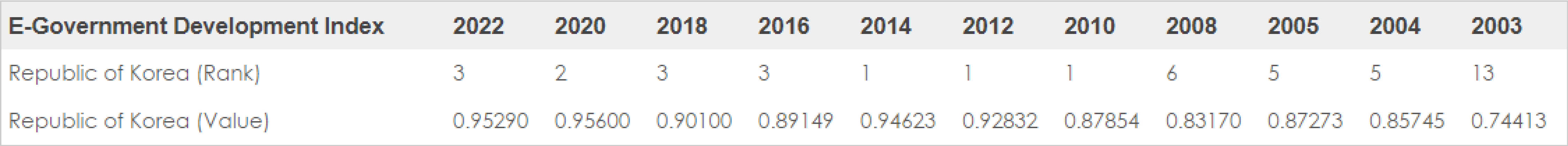
How to innovate Korean election by emerging technology

Philiph Lee

Oregon State University

Why I chose this topic

- IT Governance in ROK (Two key body: MSIT vs MOIS)
- Background of e-Government in Korea



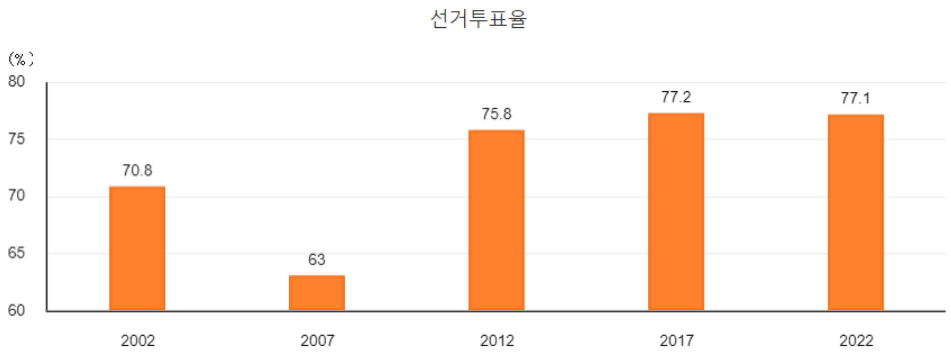
E-Government Development Index	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Republic of Korea (Rank)	3	2	3	3	1	1	1	6	5	5	13
Republic of Korea (Value)	0.95290	0.95600	0.90100	0.89149	0.94623	0.92832	0.87854	0.83170	0.87273	0.85745	0.74413

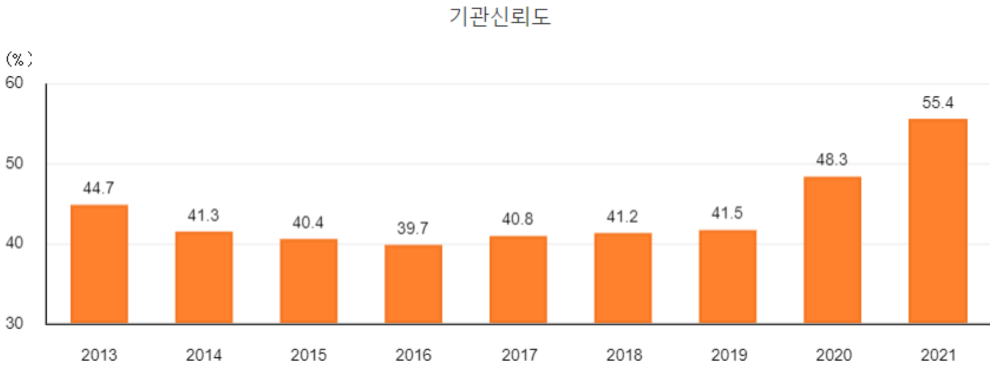
Source: UN Department of Economic and Social Affairs

MSIT: Ministry of Science and ICT
MOIS: Ministry of the Interior and Safety

Goals for this project

- Election is the cornerstone of democracy
- To increase both trust rate and election turnout rate
- To reduce unnecessary social costs
- By e-Voting, these problems can be solved.





- This is the reason why we study about the e-Voting.

Background of electronic voting

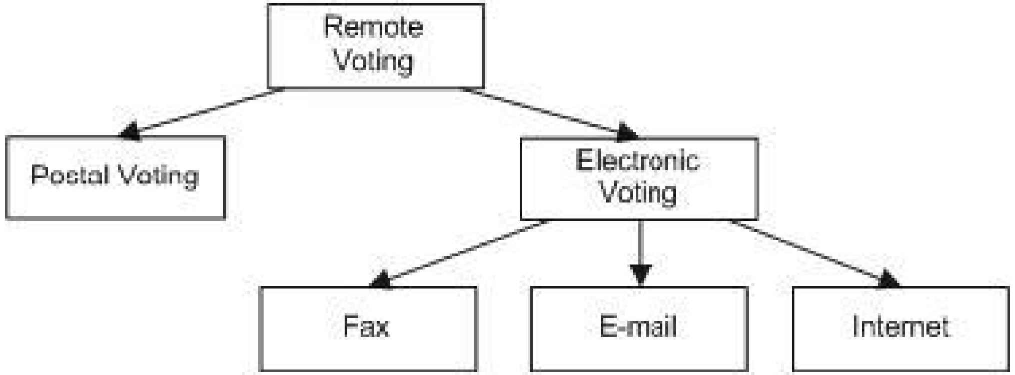


Fig. 1. Classification of remote voting channels

Source: Remote Voting Schemes: A Comparative Analysis, Jordi Puiggali and Victor Morales-Rocha

- Conceptual definition
- Classification by technology (Offline vs Online)

<Offline>

Direct voting (In-person voting method)

- Automatically tallying or Voting without a ballot paper (Except Remote Voting)
- The voter needs to visit the ballot station.

Postal Voting

- One of traditional voting method by Postal delivery.

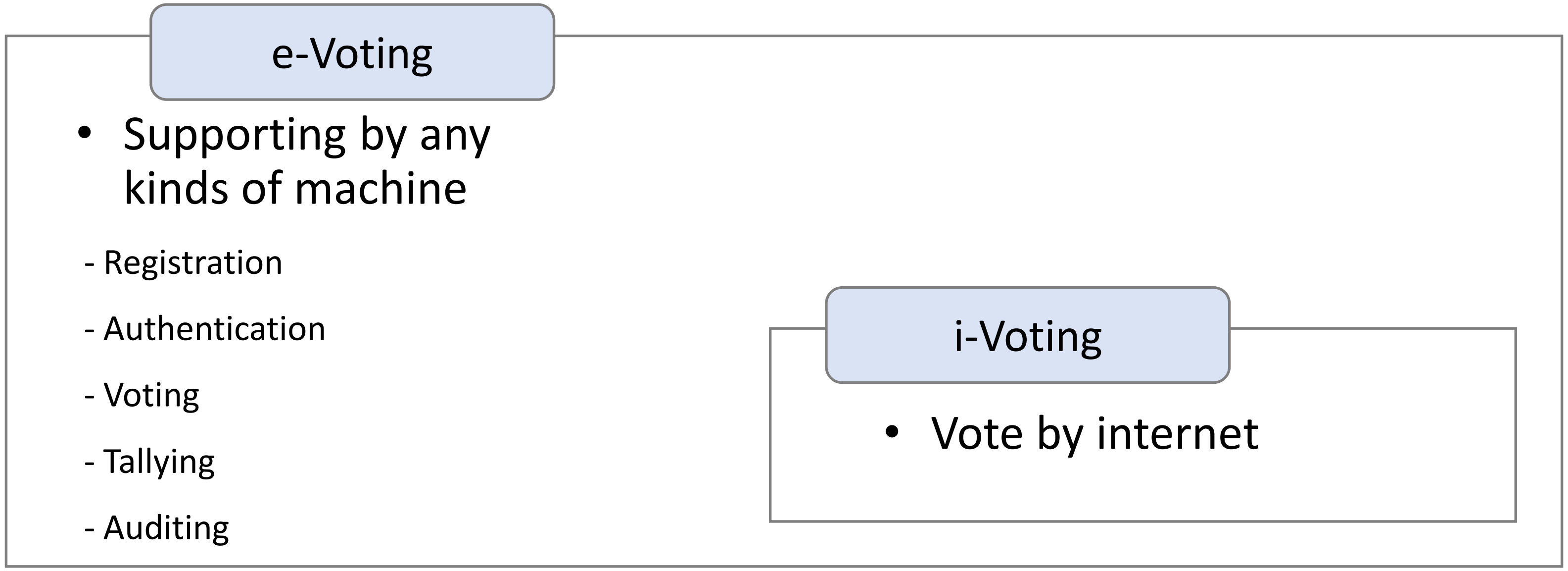
<Online>

Electronic Voting (Internet Voting as known as i-voting)

- Without restrictions on location and time.
- Online voting is one of Remote voting.

e-Voting ≠ i-Voting

i-Voting is just one of method in e-Voting. Thus, there are some country opposing to i-Voting but not for e-Voting.



e-Voting

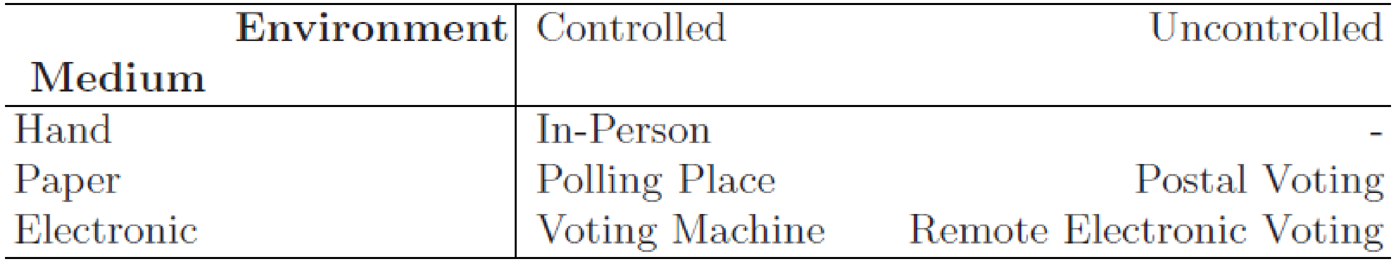
- Supporting by any kinds of machine

- Registration
- Authentication
- Voting
- Tallying
- Auditing

i-Voting

- Vote by internet

Otherwise, Some scientists separate these two by whether they are controlled or not.



Environment **Medium**	Controlled	Uncontrolled
Hand	In-Person	-
Paper	Polling Place	Postal Voting
Electronic	Voting Machine	Remote Electronic Voting

Source: The Development of Remote E-Voting Around the World: A Review of Roads and Directions: Robert Krimmer, Stefan Triessnig, and Melanie Volkamer

Why do we need e-Voting (Pros vs Cons)

- Do we need to consider e-Voting?
- If it is, how about i-Voting?

Benefits		Disadvantages	
Ability to Deal with Complex Elections		Lack of Transparency	M
Accessibility		Confidence	M
Less Polling Staff		Audit of Results	M
Elimination of Invalid/Incorrectly Cast Ballots		Secrecy of the Ballot	M
Speed of Counting		Setup Procedures for Electronic Voting Machines	
Standard Adjudication of Ballots		Tendered Ballots	M
Accurate Tabulation of Results		Consequences of Breakdown	M
Fraud Prevention		Confusion for Illiterate/Uneducated Voters	
		Specialized IT Skills	
		Integrity and Accuracy of Source Code	
		Storage of Equipment	
		Power Considerations	
		Security	M
		Consequences of Fraud	M
		Management Complexity	M
		Cost	M

Source: International Experience with E-Voting, Norwegian E-vote project(2012, June)

Many risks can be mitigated compared to 2012

Requirements of electronic voting

4 major principle of election

- By law (usually in the constitution)

4 major properties of election

Accuracy

Democracy

Privacy

Verifiability

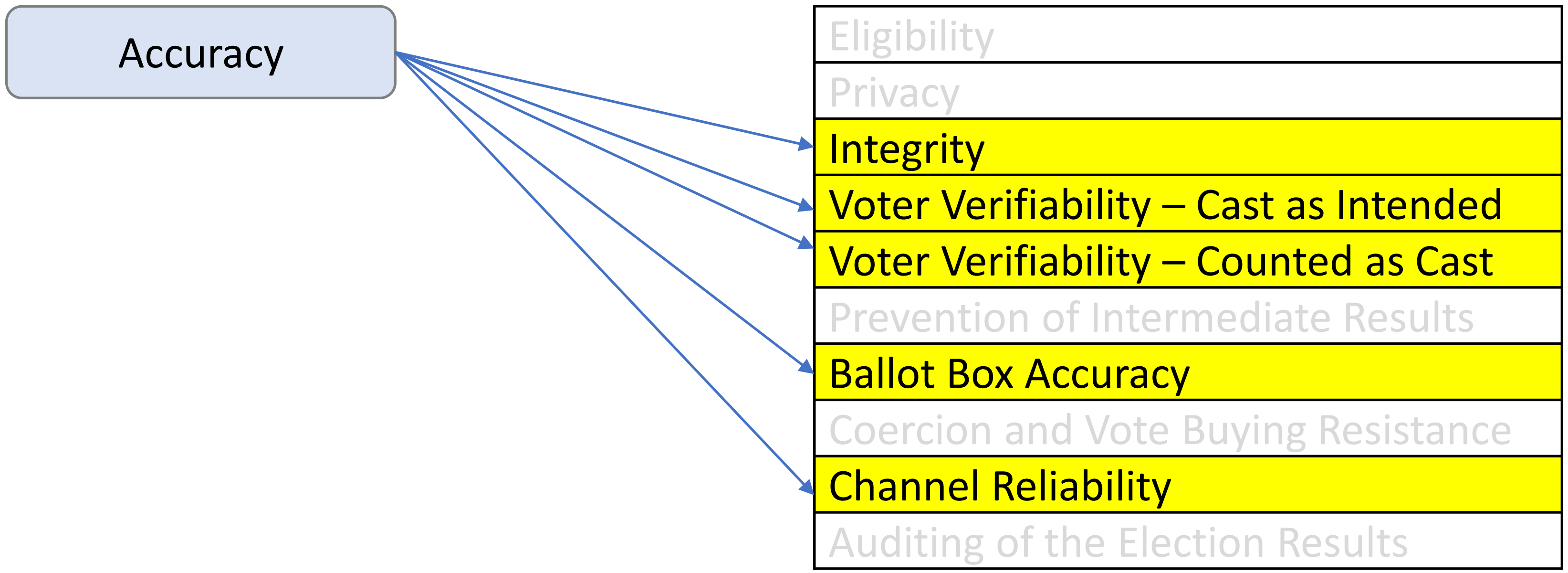
Requirements of electronic voting

1st principle of election: Accuracy

- A casting vote cannot be altered.
- An invalid vote is not counted.
- Each voter has the guarantee that his/her ballot is counted.

major properties of election

Considerable factors



Accuracy

- Eligibility
- Privacy
- Integrity
- Voter Verifiability – Cast as Intended
- Voter Verifiability – Counted as Cast
- Prevention of Intermediate Results
- Ballot Box Accuracy
- Coercion and Vote Buying Resistance
- Channel Reliability
- Auditing of the Election Results

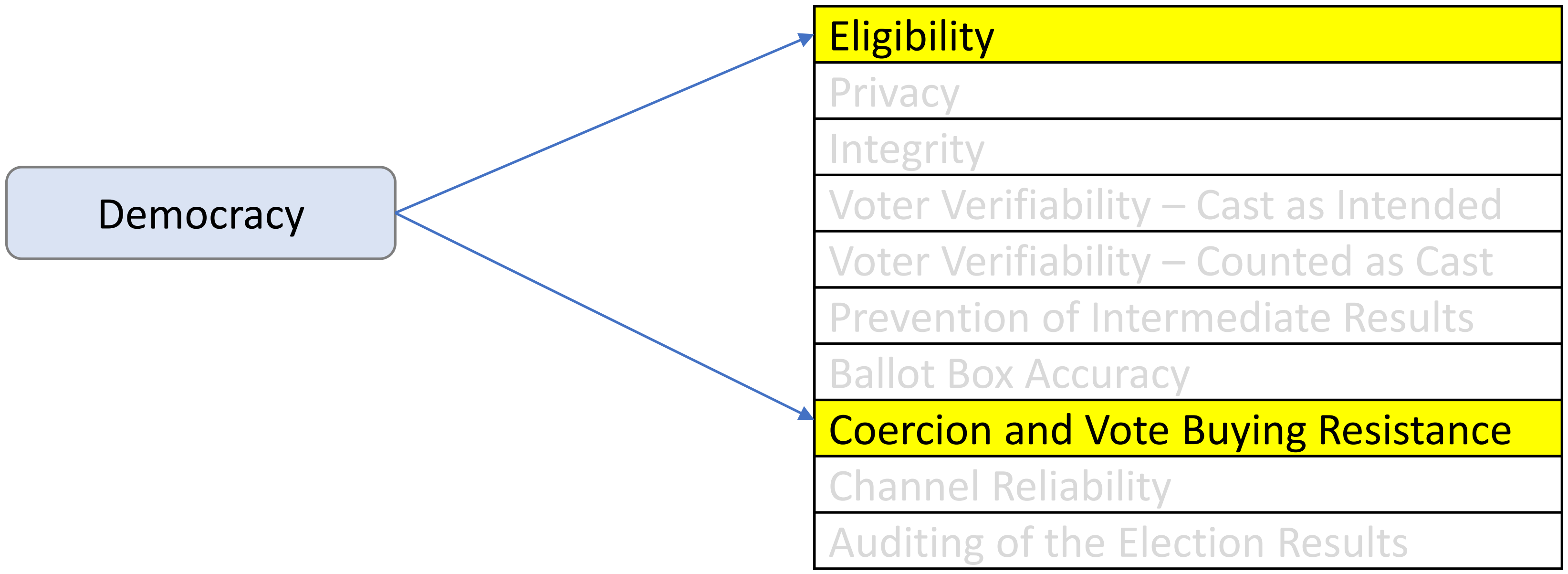
Requirements of electronic voting

2nd principle of election: Democracy

- Only an authorized voter can participate.
- Each voter can cast only one vote

major properties of election

Considerable factors



Democracy

Eligibility

Privacy

Integrity

Voter Verifiability – Cast as Intended

Voter Verifiability – Counted as Cast

Prevention of Intermediate Results

Ballot Box Accuracy

Coercion and Vote Buying Resistance

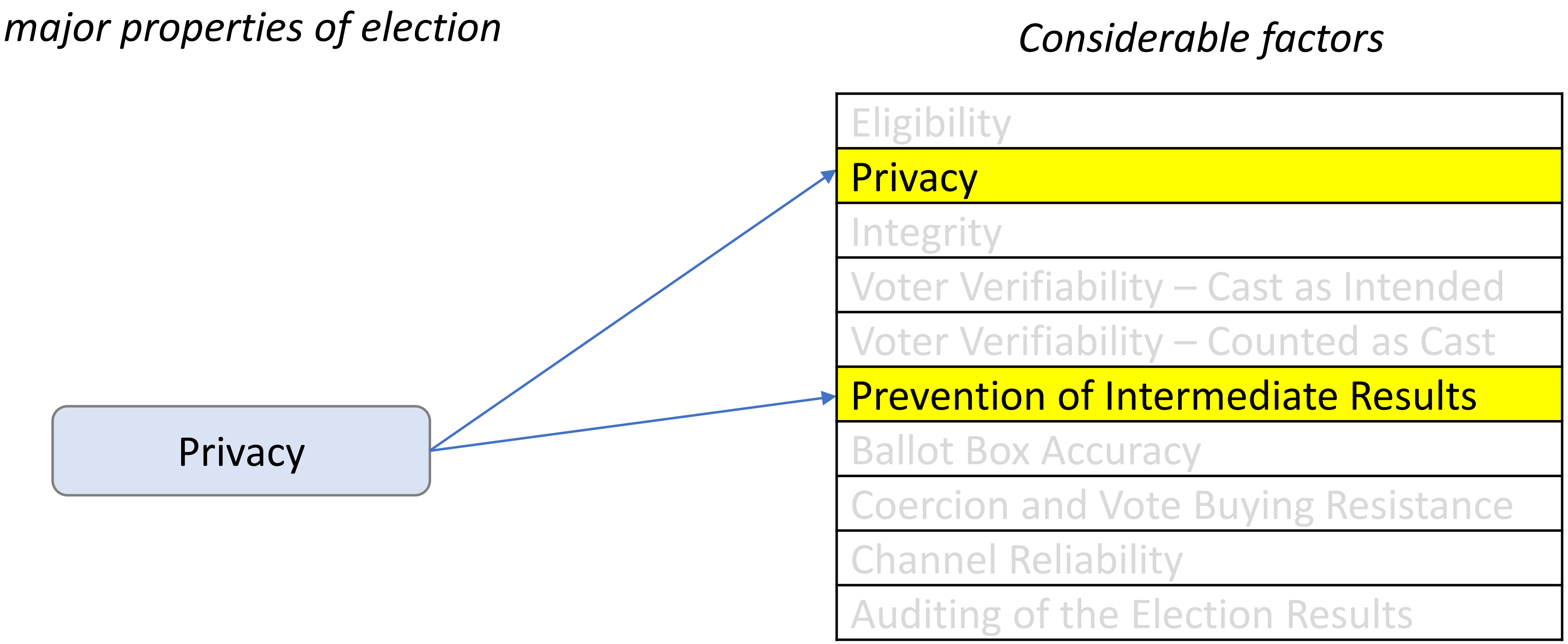
Channel Reliability

Auditing of the Election Results

Requirements of electronic voting

3rd principle of election: Privacy

- A ballot cannot be linked back to the voter who cast it.



major properties of election

Considerable factors

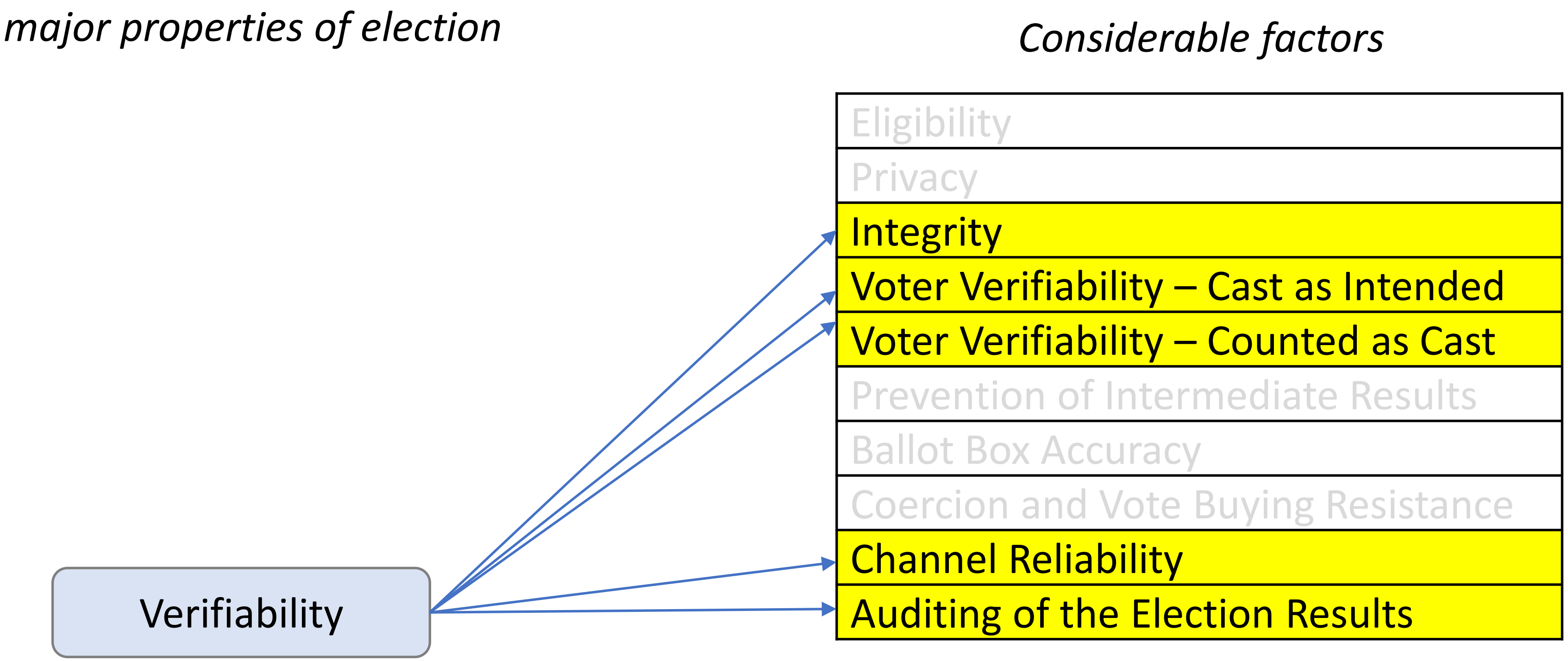
Privacy

Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results

Requirements of electronic voting

4th principle of election: Verifiability

- Each voter can verify that his/her vote is counted.
- Individual vs Universal



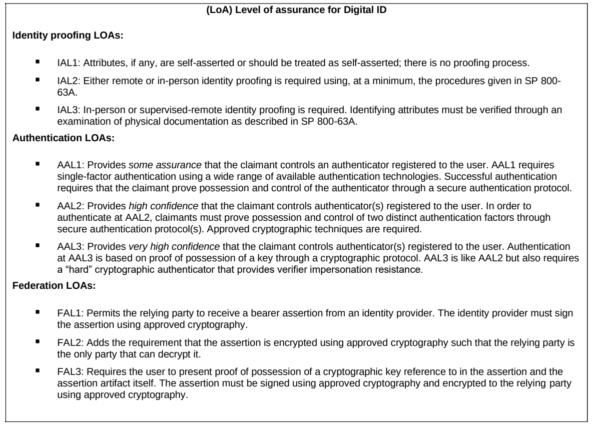
major properties of election

Considerable factors

Verifiability

Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results

1. Authentication



(LoA) Level of assurance for Digital ID

Identity proofing LOAs:

- IAL1: Attributes, if any, are self-asserted or should be treated as self-asserted; there is no proofing process.
- IAL2: Either remote or in-person identity proofing is required using, at a minimum, the procedures given in SP 800-63A.
- IAL3: In-person or supervised-remote identity proofing is required. Identifying attributes must be verified through an examination of physical documentation as described in SP 800-63A.

Authentication LOAs:

- AAL1: Provides *some assurance* that the claimant controls an authenticator registered to the user. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- AAL2: Provides *high confidence* that the claimant controls authenticator(s) registered to the user. In order to authenticate at AAL2, claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.
- AAL3: Provides *very high confidence* that the claimant controls authenticator(s) registered to the user. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

Federation LOAs:

- FAL1: Permits the relying party to receive a bearer assertion from an identity provider. The identity provider must sign the assertion using approved cryptography.
- FAL2: Adds the requirement that the assertion is encrypted using approved cryptography such that the relying party is the only party that can decrypt it.
- FAL3: Requires the user to present proof of possession of a cryptographic key reference to in the assertion and the assertion artifact itself. The assertion must be signed using approved cryptography and encrypted to the relying party using approved cryptography.

Standards: eIDAS, ISO/IEC 29115, NIST 800-63-3

- Definition: *Only voters eligible to vote who are unequivocally identified and authenticated by the voting system may cast a vote*

By de-facto-standards, there are level of authentication

Level 1 **(Low)**	**1 factor authentication:** Memorized secret(Password) Look-up secret(Security Card) Out of band OTP device Cryptographic S/W(Certificate such as PKI)
Level 2 **(Substantial)**	**2 factor authentication** Multi-factor level1 (OTP with Pin code)
Level 3 **(High)**	**3 factor authentication** Multi-factor device + Memorized Secret

For e-Voting, Level3 is strongly recommend.
i.e) France : App “Franceconnect” (X)

2. Privacy

- Definition: *The voting system has to protect voter privacy, concealing the relation between voter and his/her cast vote, and ensuring that the voter's choice will remain anonymous.*

	Paper voting	Electronic Voting	Internet Voting
Privacy	Set up compartmentalized polling places and partitions If you do not fold it invisibly, it may be invalidated.	Physical access control same as Paper Voting + The emission signal should not be leaked from the voting machine aka the Side channel. The voting machine should be offline and blocked to a USB drive. <VVPAT: Voter Verified Paper Audit Trail> When printing out the voting result contents need to be not recognizable by humans. Thus, the Barcode of QR code was used.	Encrypted by the public key of the Election agency. Thus, only the Election agency can decrypt votes data. After voting, voters' id (profile) and the voting result were separated and stored in a different location for safety.

3. Integrity

- Definition: *A voting system has to protect the vote against manipulation once it is cast and until it is counted*

	Paper voting	E-voting	i-Voting
Integrity	The risk of manipulating results: direct access to the ballot box. The impact is relatively small.	No network connection of the voting machine was guaranteed for integrity. But by taking control of tallying server, The impact is huge. To mitigate risk, let's print every voting and gathering. ➔ VVPAT (Voter Verified Paper Audit Trail) Can reconcile the paper and tally counts by ballot box machine.	Use a double envelope, every vote is encrypted by the voters' private key (Digital signing) and the election agency's public key(Privacy) But by cyber attack, The impact is extremely huge. <Estonia> The data is stored on DVD to prevent tampering. Is this enough even though the risk is much higher?

4. Traceability

- *Traceability have two point of views. (Individual vs Universal verification)*

- **Individual verification** : voter must have the possibility to check that his/her vote has been accurately recorded.

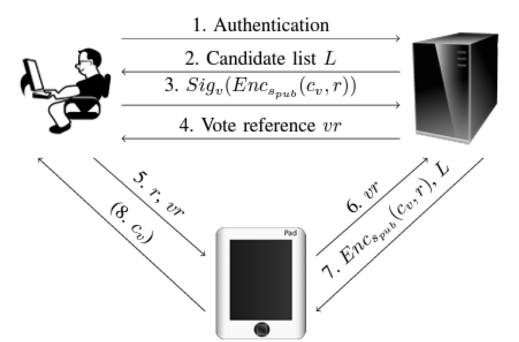


Fig. 2. The Estonian Internet voting protocol with vote verification

Trace method in Estonian I-Voting system

Sending the result from PC to Mobile phone (Corresponding No.5 on the left)

When the voter votes by i-Voting, it is encrypted with a public key (r) randomly generated by the server and transmitted to the server. When the vote is reflected, a random number (vr) is returned. By recognizing the combined QR code on the smartphone, the voter can decrypt and check the voting contents.

- **Universal verification** : voters must have the possibility to verify the inclusion of his/her vote in the final tallying.

Only need to check whether the voters’ vote is applied to tally

4. Traceability

- *Depending on law, individual verification was not allowed in most countries.*

“a remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast” (Council of Europe 2004: Recommendation 51).

	Paper Voting	Individual Verification	Universal Verification
Traceability	Not supported.	<Estonia> Support the individual verification After voting, the voters can see what they select by mobile device. <Begium > Limited the individual verification Before leaving the ballot station, the voter can see their result on the voting machine. <US> Limited the individual verification After voting, what the voters do is printing out.	After voting, the voter can see whether they vote or not. For ideal universal verification, Need to show that my vote is applied to tally!

5. Prevention of Intermediate Results

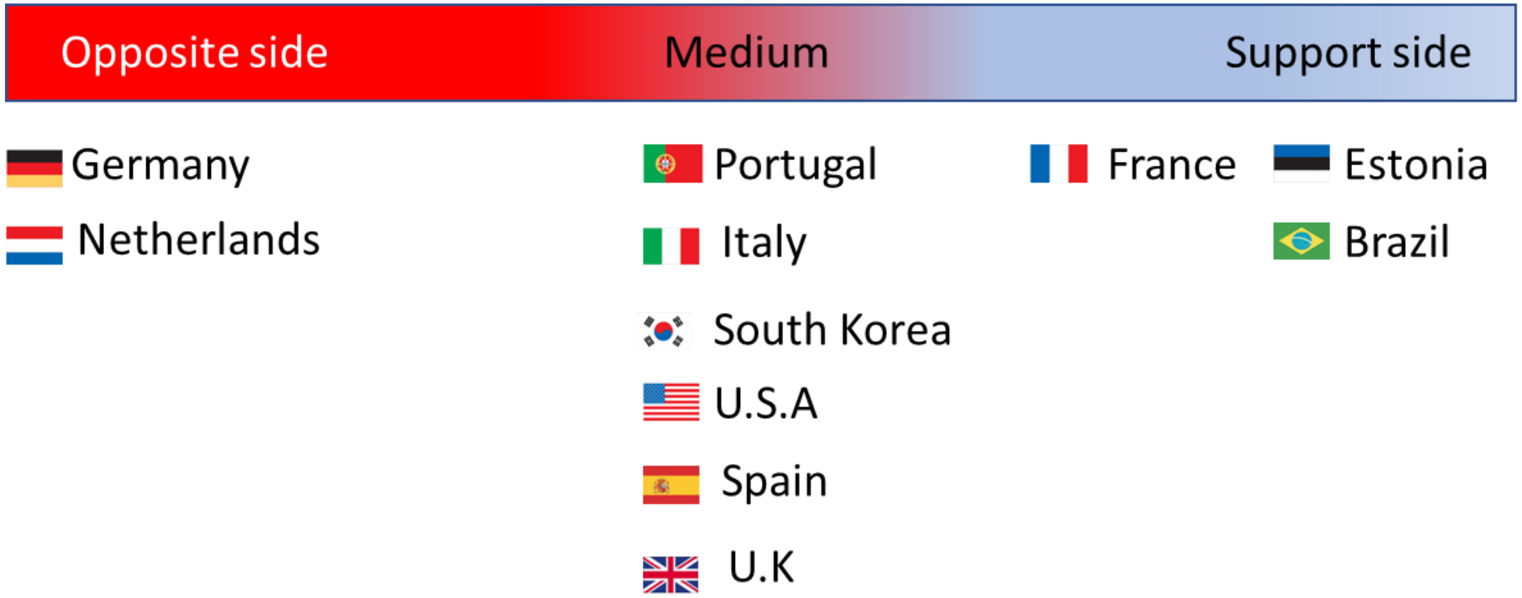
prevent the disclosure
of intermediate results before the election is closed

6. Auditing of the Election Results

All process can be audited by human resources

World cases on i-Voting

- The position about i-voting (Negative vs Positive)



Opposite side

Medium

Support side

Germany

Netherlands

Portugal

Italy

South Korea

U.S.A

Spain

U.K

France

Estonia

Brazil

- Opposite side: Done pilot project or study i-Voting and enact the law not to allow it
- Medium: Done pilot project or study but hold
- Support side: Partially adapt i-Voting to election (France only for oversea citizen) or totally covered

All elections by Internet (Estonia)

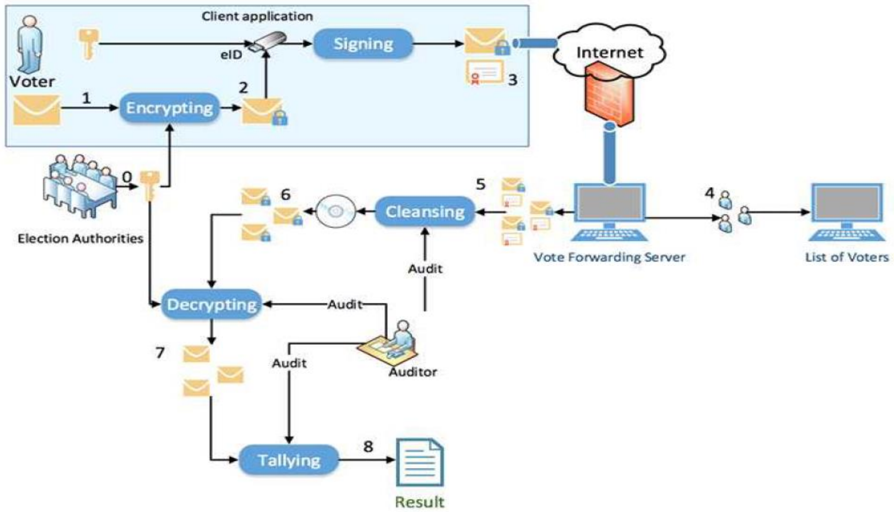
- i-Voting on every national election
- Use of e-ID
- Double envelope
- Guarantee the Individual verification

(Point) Allow to vote multiple times

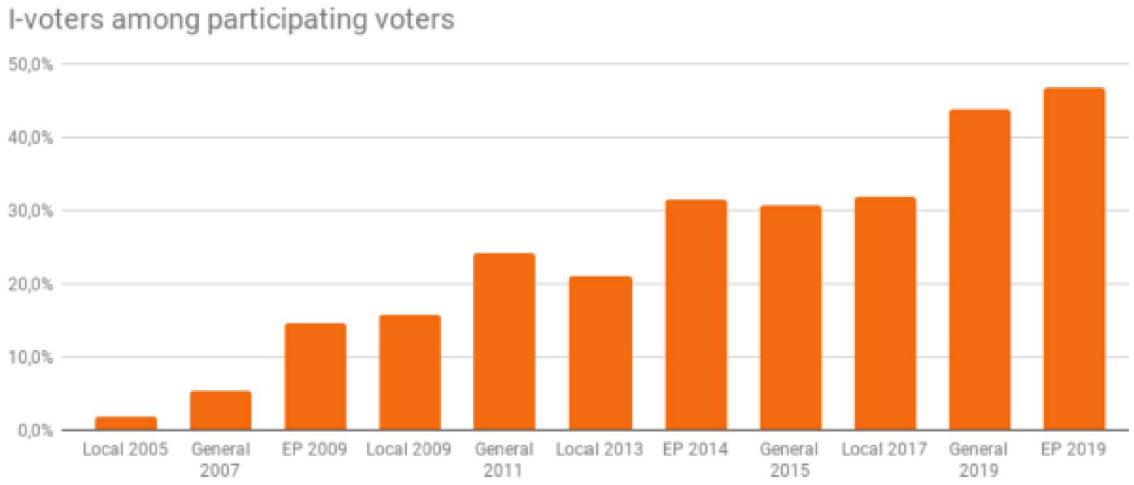
Why!

To reduce costs due to limited resources : After independence from the Soviet Union in 1991, the Estonian gov needs to reduce costs.

EESTI VABARIIK Republic of Estonia DIGITAALNE ISIKUTUNNISTUS Digital Identity Card ERÇETIN MANI ÖZER 36908209993 US1234567 02 08 2018 02 08 2023 145478 SPECIMEN Source: politsei.ee	 Source: https://producement.com/
Estonia e-ID	Insertion to PC for authentication

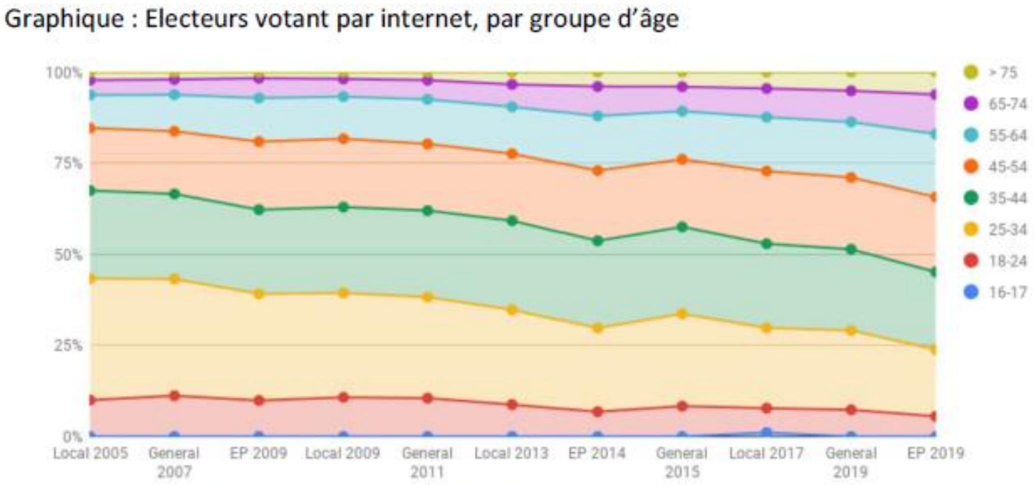


All elections by Internet (Estonia)



I-voters among participating voters

Source: https://www.valimised.ee/en/archive/previous-elections



Graphique : Electeurs votant par internet, par groupe d'âge

Source: https://www.valimised.ee/en/archive/previous-elections

High turn-out rate.

The informatization gap can be covered!

The ratio of using i-Voting in 65-74 and older more than 75 was doubled during this period.

Some elections by Internet (France)

- Overseas voter (1.8milion) > entire Estonian

(Point) There are multiple rounds

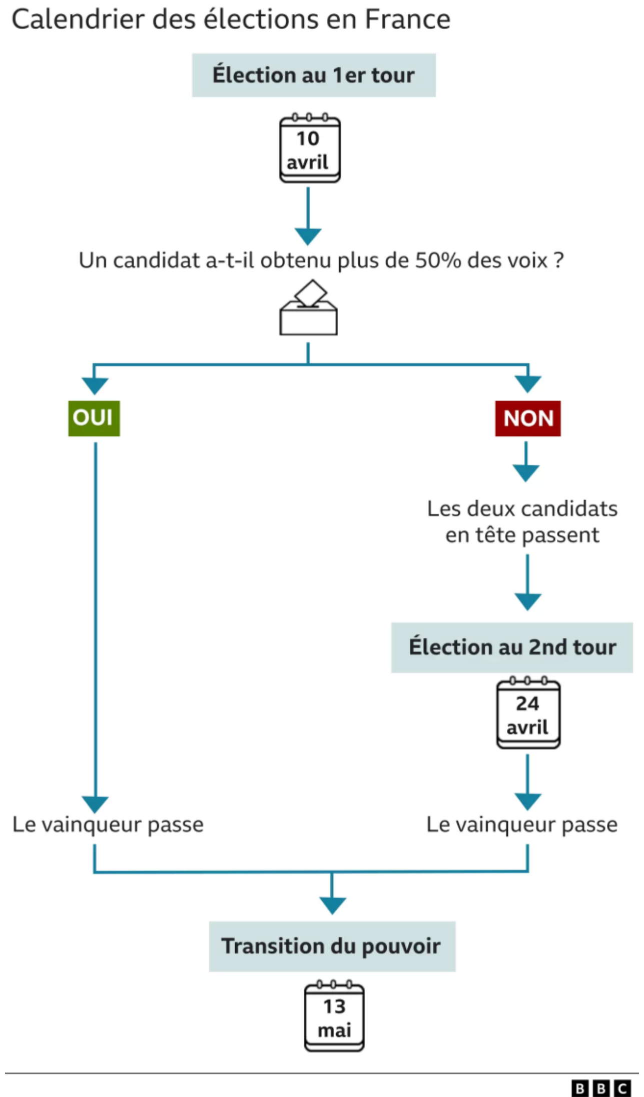
Why!

In a French election, the voter needs to visit many times.

2 times voting was needed for the presidential election.
At 1st vote, two major candidates were chosen.
At 2nd Vote, voters should vote again for two major candidates.

And there was an accident of postal voting in 2017.

- the postal ballot bag was left at the airport for several days.
- All votes were invalidated.
- France proposed an amendment to ban postal voting for overseas citizens.

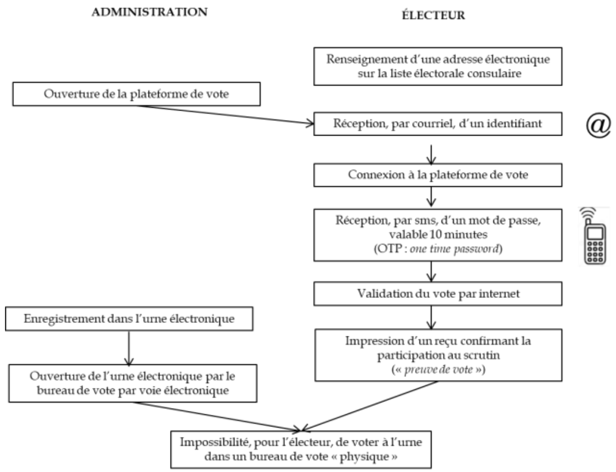


Some elections by Internet (France)

- How to divide into voters by their environment

Direct voting for Domestic voters

Internet voting for overseas voters



ADMINISTRATION

ÉLECTEUR

Renseignement d'une adresse électronique sur la liste électorale consulaire

Ouverture de la plateforme de vote

Réception, par courriel, d'un identifiant

@

Connexion à la plateforme de vote

Réception, par sms, d'un mot de passe, valable 10 minutes (OTP : *one time password*)

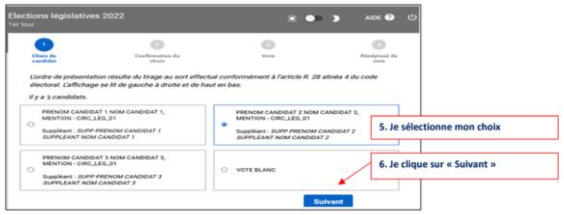
Validation du vote par internet

Enregistrement dans l'urne électronique

Impression d'un reçu confirmant la participation au scrutin (« *preuve de vote* »)

Ouverture de l'urne électronique par le bureau de vote par voie électronique

Impossibilité, pour l'électeur, de voter à l'urne dans un bureau de vote « physique »



Elections législatives 2022
1er tour

L'ordre de présentation résulte du tirage au sort effectué conformément à l'article R. 28 alinéa 4 du code électoral. L'affichage se lit de gauche à droite et de haut en bas.

Il y a 3 candidats.

○ PRENOM CANDIDAT 1 NOM CANDIDAT 1, MENTION - CIRC_LEG_01
Suppléant : *SUPP PRENOM CANDIDAT 1 SUPPLEANT NOM CANDIDAT 1*

● PRENOM CANDIDAT 2 NOM CANDIDAT 2, MENTION - CIRC_LEG_01
Suppléant : *SUPP PRENOM CANDIDAT 2 SUPPLEANT NOM CANDIDAT 2*

○ PRENOM CANDIDAT 3 NOM CANDIDAT 3, MENTION - CIRC_LEG_01
Suppléant : *SUPP PRENOM CANDIDAT 3 SUPPLEANT NOM CANDIDAT 3*

○ VOTE BLANC

Suivant

5. Je sélectionne mon choix

6. Je clique sur « Suivant »

ID = by Email
Password = by SMS

Is it enough?
About 15% was a loss for the connection.

Estonia vs France

- Why did these two countries make a different decision? (entire i-voting)

	Estonia	**France**
Population(Voter)	**887,420** (1,303,798)	**48,589,606** (65,480,710)
Oversea	About 80000	1.4million
Turnout(%)	63.67%	46.23%

- **The number of voters**: the overseas voters in France is high.

- **The position of internet voting**: France was stopped for a while

  In 2017, the Cazeneuve French government decided to suspend votes through the internet for cyber security risks. And 2022 internet voting was appeared again only for oversea citizen.

- **Political difference**

  The progressives got to gain from e-Voting

  In Korea, it was postal voting.

Progressive

Conservative

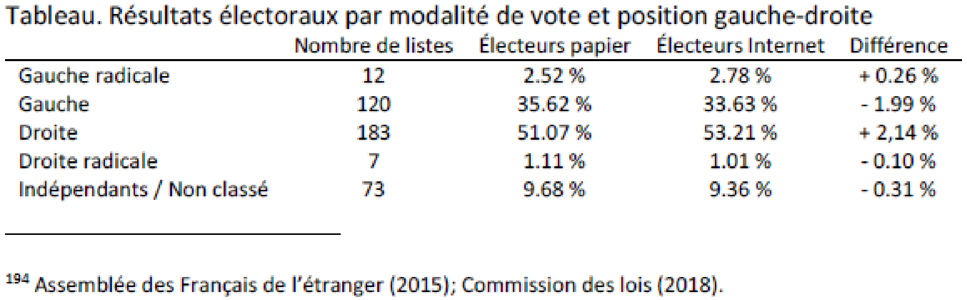


Tableau. Résultats électoraux par modalité de vote et position gauche-droite

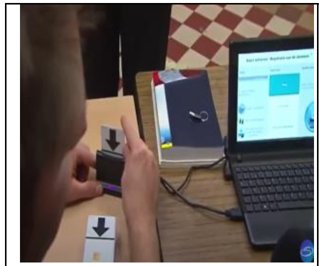
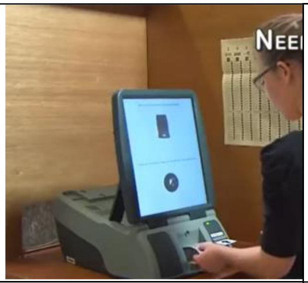
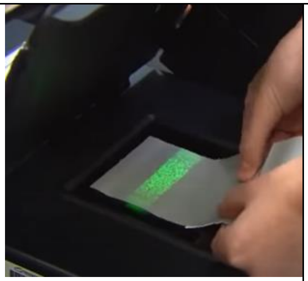
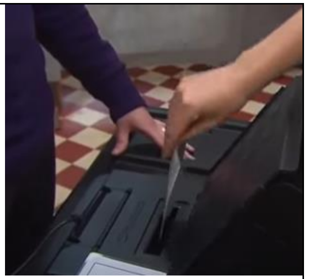
	Nombre de listes	Électeurs papier	Électeurs Internet	Différence
Gauche radicale	12	2.52 %	2.78 %	+ 0.26 %
Gauche	120	35.62 %	33.63 %	- 1.99 %
Droite	183	51.07 %	53.21 %	+ 2,14 %
Droite radicale	7	1.11 %	1.01 %	- 0.10 %
Indépendants / Non classé	73	9.68 %	9.36 %	- 0.31 %

[194] Assemblée des Français de l'étranger (2015); Commission des lois (2018).

Not internet but electronic election **for Vote** (Belgium, U.S.A)

- Difference between Belgium and U.S:

  - Smart card, VVPAT (Not for all states in U.S)

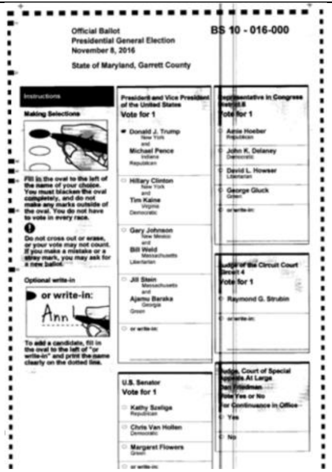
			
Step1: Receiving smart card after identification	Step2 : Insert into Voting machine and printed out the result	Step3: Scanning the result to ballot box machine	Step4: Submitting the paper after scanning the machine

Why!

1. Why voting machine separate from ballot box machine? Voting machine should not connect to network for security.
2. Why printing paper? It called as VVPAT(Voter-verified paper audit trail). By law(by country), need to audit by human one by one. In Washington D.C in 2018, Hearing was in held, it was reported that 5 states in US still doesn't need VVPAT for e-Voting.
3. Why to use Smart card : To protect anonymity of voter inside polling station.

Not internet but electronic election **only for Tallying** (U.S.A)

- Optical Scan voting is still major method in the U.S election.



Official Ballot
Presidential General Election
November 8, 2016
State of Maryland, Garrett County

BS 10 - 016-000

Instructions

Making Selections

Fill in the oval to the left of the name of your choice. You must blacken the oval completely, and do not make any marks outside of the oval. You do not have to vote in every race.

Do not cross out or erase, or your vote may not count. If you make a mistake or a stray mark, you may ask for a new ballot.

Optional write-in

or write-in: Ann

To add a candidate, fill in the oval to the left of "or write-in" and print the name clearly on the dotted line.

President and Vice President of the United States
Vote for 1

● Donald J. Trump New York and Michael Pence Indiana Republican
○ Hillary Clinton New York and Tim Kaine Virginia Democratic
○ Gary Johnson New Mexico and Bill Weld Massachusetts Libertarian
○ Jill Stein Massachusetts and Ajamu Baraka Georgia Green
○ or write-in:

U.S. Senator
Vote for 1

○ Kathy Szeliga Republican
○ Chris Van Hollen Democratic
○ Margaret Flowers Green
○ or write-in:

Representative in Congress District 6
Vote for 1

○ Amie Hoeber Republican
○ John K. Delaney Democratic
○ David L. Howser Libertarian
○ George Gluck Green
○ or write-in:

Judge of the Circuit Court Circuit 4
Vote for 1

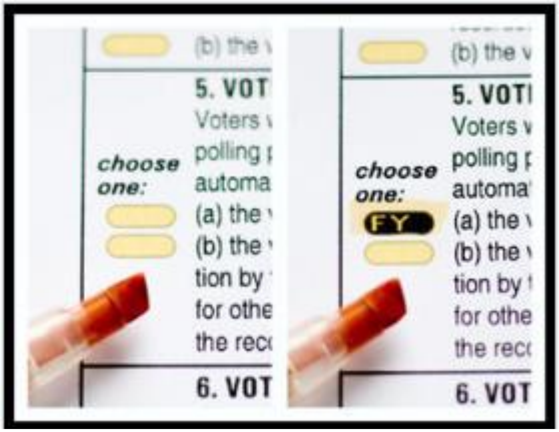
○ Raymond G. Strubin
○ or write-in:

Judge, Court of Special Appeals At Large
Dan Friedman
Vote Yes or No
For Continuance in Office

○ Yes
○ No

Source: Wikipedia

Optical Scanning Voting System



Scantegrity

Why!

- The position of i-voting: the United States is skeptical. The Russian cyber threat in the 2016 presidential election.

Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet (Voter Registration and Voter Registration Databases)

Learn from failure …

- Netherland (pilot project) : Detection of voting machine signals at 40 meters outside the polling place, unauthorized use of some unauthorized software versions, unable to audit by humans (Blackbox)

  ➔ Should consider countermeasures for these risks.

- Swiss (pilot project): Use ZKP* to authenticate but failed.

  * the date of birth of the voter and the municipality of origin of the voter

  ➔ Should not use ambiguous identifiers

- Estonia (2015 election): By system failure including the backup server, some votes were lost.

  ➔ Should setup a complete backup plan

- Misbelief for losing confidentiality: Hiding source code of e-Voting system. It was regarded as a black box. This is an issue for transparency.

  ➔ Should open the source code to the public for safety

Suggestion e-Voting for Korea

- Legal analysis

Public Official Election Act

Article 146 (Method of Election)

(1) An election shall be made by **a vote marked on the ballot papers**.

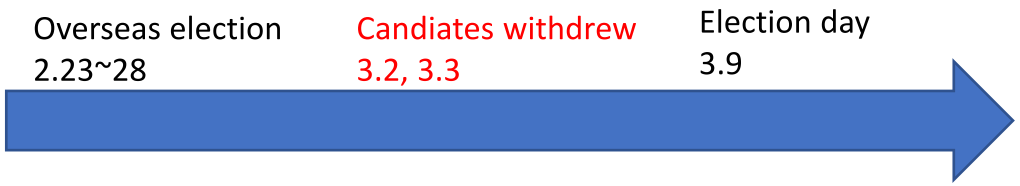
(2) **A vote shall be made in person or by mail**, and one person shall be entitled to one vote…

By law, only in person or by mail are allowed

Suggestion e-Voting for Korea

- Limitation on 2022 presidential election

Limitation
 - Before a week of election-day, 2 candidates withdrew. For the result, many invalid votes were appeared.



Overseas election
2.23~28

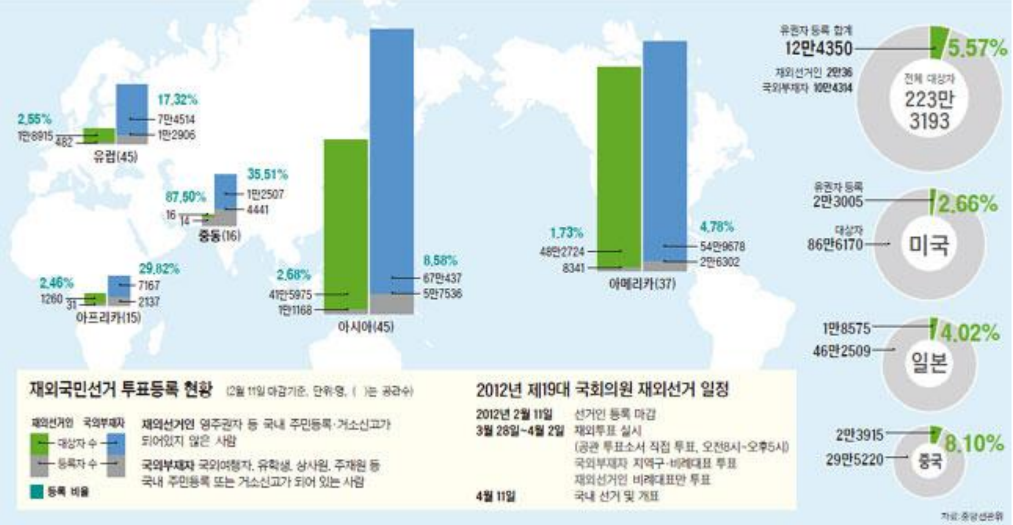
Candiates withdrew
3.2, 3.3

Election day
3.9

Need to reduce invalid votes

Suggestion e-Voting for Korea

- Current oversea voting needs to be changed for low turnout rate and high voting cost.



재외국민선거 투표등록 현황 (2월 11일 마감기준, 단위:명, ( )는 공관수)

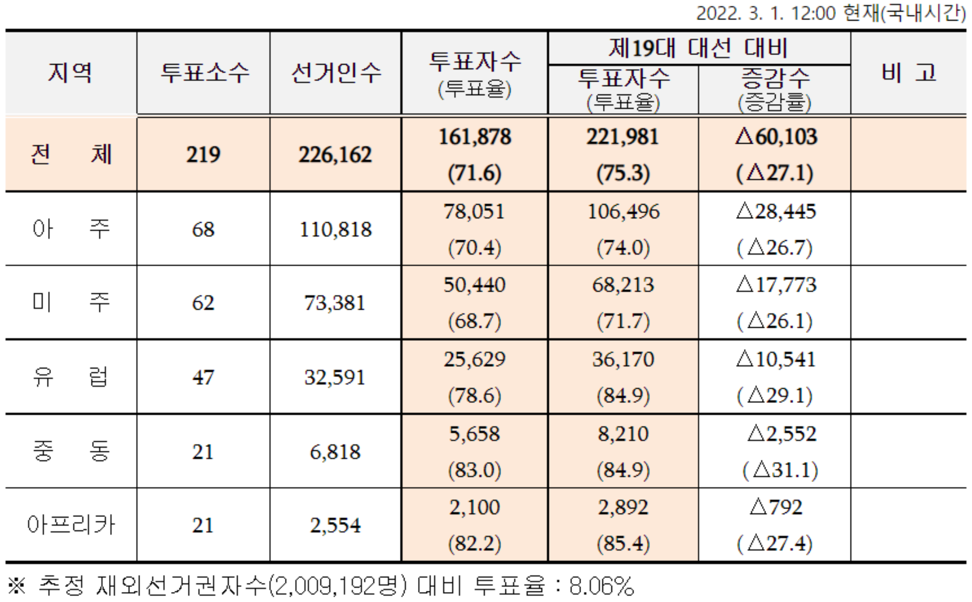
재외선거인 영주권자 등 국내 주민등록·거소신고가 되어있지 않은 사람

국외부재자 국외여행자, 유학생, 상사원, 주재원 등 국내 주민등록 또는 거소신고가 되어 있는 사람

2012년 제19대 국회의원 재외선거 일정

2012년 2월 11일	선거인 등록 마감
3월 28일~4월 2일	재외투표 실시 (공관 투표소서 직접 투표, 오전8시~오후5시) 국외부재자 지역구·비례대표 투표 재외선거인 비례대표만 투표
4월 11일	국내 선거 및 개표

Source : JoongAng daily news. 2012.03.04



2022. 3. 1. 12:00 현재(국내시간)

지역	투표소수	선거인수	투표자수 (투표율)	제19대 대선 대비		비 고
				투표자수 (투표율)	증감수 (증감률)	
전 체	219	226,162	161,878 (71.6)	221,981 (75.3)	△60,103 (△27.1)	
아 주	68	110,818	78,051 (70.4)	106,496 (74.0)	△28,445 (△26.7)	
미 주	62	73,381	50,440 (68.7)	68,213 (71.7)	△17,773 (△26.1)	
유 럽	47	32,591	25,629 (78.6)	36,170 (84.9)	△10,541 (△29.1)	
중 동	21	6,818	5,658 (83.0)	8,210 (84.9)	△2,552 (△31.1)	
아프리카	21	2,554	2,100 (82.2)	2,892 (85.4)	△792 (△27.4)	

※ 추정 재외선거권자수(2,009,192명) 대비 투표율 : 8.06%

- **Low turnout rate**: In 2022, the turnout was 71.6% but only 8.05% of voters were registered.
- **Restrictions on the promotion of participation in Elections**: Not in democratic countries
- **High election cost for overseas voting**: In 2012, only 5.57% of voters were registered while 22 million USD in spending (The Cost per voter)

The requirements for Korea e-Voting

- Can found major requirements for e-Voting from Korean laws (Constitution, Public Officer Election Act)

Seq		Election requirements by Laws	Corresponding factors
Mandatory	1	선거인명부는 비밀, 무결 하게 관리되어야 함(보통원칙) The master file must be kept secret and integrity (One of 4 principles of elections)	Privacy
	2	유권자 1인 당 1표가 행사되어야 함(평등원칙) Only one vote for one voters should be assigned (One of 4 principles of elections)	Eligibility Coercion and Vote Buying Resistance
	3	투표는 유권자 본인이 직접해야함(직접원칙) Proxy voting was not allowed to the elections (One of 4 principles of elections)	Eligibility
	4	기표 내용은 비밀이 보장되어야 함 (Confidentiality비밀원칙) What the voter did must be kept secret (One of 4 principles of elections)	Privacy
	5	투표시 조작되지 않아야 함 The voting must not have tampered.	Voter Verifiability – Cast as Intended
	6	개표집계가 조작되지 않아야 함 The tallying must not have tampered.	Voter Verifiability – Counted as Cast
	7	투표용지는 정확하게 선거인명부와 일치해야 함 The ballot should match the master file of voters.	Integrity
	8	개표전까지 집계내용이 공개되어서는 안됨 The tallying result must be kept secret before finishing voting.	Prevention of Intermediate Results.
	9	투표지가 분실되어서는 안됨 The ballot must not be lost.	Channel Reliability
	10	집계는 감사가 가능해야 함 (Auditability) The tallying must be enabled to audit (verify) by humans.	Auditing of the Election Results
	11	선거관리는 동등한 수준에서 관리되어야 함 The election should be controlled by the same level of control.	Channel Reliability
	12	정해진 기간에 투표가 지속 가능해야함 During the election period, voting should not be interrupted or stopped.	Channel Reliability
Optional	13	본인 투표 결과를 추적 가능해야 함 (Traceability) The voters need to trace what they vote from voting to tallying	New
	14	정확한 선거 상황이 투표시점에 반영되어야 함(후보 사퇴 등) The recent election content needs to be applied on voting.	N/A

Learn from cases

- Many risks are found in models in use in other countries, and some are not allowed by Korean law.

Cases	Considerable Factor	Risks
Estonia i-Voting	For authentication, Use e-ID and Pin code With writing DVD media, it kept the integrity Trace what the voter vote after voting	Still possible of stealing the identity The server to write DVD can be attacked and malfunction The violation of Vote-buying and vote by coercion by Korean Law
France oversea internet voting	Authenticate by SMS and email	The plaintext from SMS and email can be leaked outside the border of country
US e-Voting	Some states doesn’t necessary VVPAT Even with VVPAT, the selection of voter printed out the paper with Barcode or QR Use of machine that manufacture in US	The violation of enabling to verify by humans. What the voter votes can be leaked inside the polling station. If we consider internet voting, it’s difficult to limit only domestic manufacturing.

We Need a different model for Korean election

The design of Korean election system

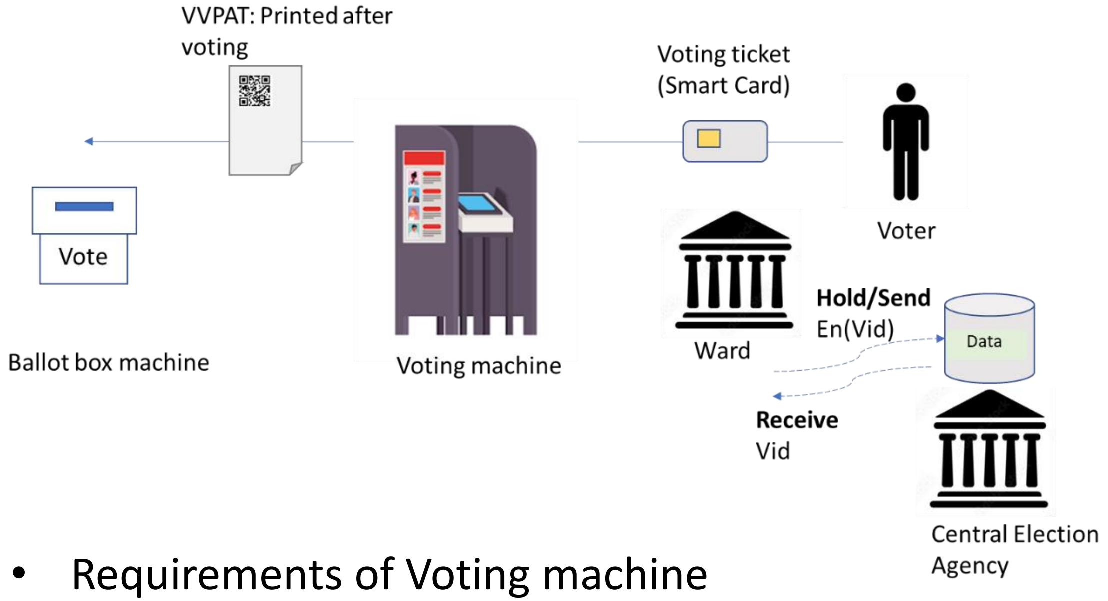
- Divides into two parts
- E-Voting is for domestic voters
- i-Voting is for overseas voters

	Domestic Voters	Overseas Voters
Voters	44,197,692 (Total)	226,162 (registered in 2.3million)
Period	Main election day	Before a week election day
Method	Direct(In-person) and mail	Direct and internet
Register	By government	By request of registration
Tallying	Tallying after voting	Same day with e-Voting
Authentication	By showing ID	By using e-Passport
Risk Management Goal	Elimination (Voting machine should be offline. VVPAT is mandatory)	Mitigation (Separation of data (Voter ID and vote) Stored in Blockchain)

In 2022 Presidential election

Korean e-Voting model (Offline)

- In-person(=Direct) voting with Voting machine.



- Requirements of Voting machine

- DRE with VVPAT, Enables tallying and audit by humans.
- For entrance, check whether the voter is valid or not.

Why!

1. Why do we need to print the vote?
 - Illegal if humans can't audit tallying by the Supreme Court precedent in Korea (2016. 3. 31. 2015헌마1056·1172, 2016헌마37(병합)

2. Why do we need Smart cards?
 - To provide the anonymity of voters inside the Polling station.

Korean e-Voting model (Offline)

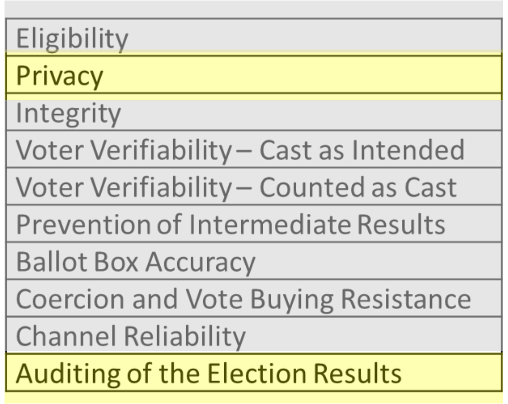
Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results

Election Procedure

1. The voter enters to the polling station, Shows his/her identification card
2. Election Government Officer(EGO) checks the validity, If it’s valid, give the smart card to the Voter
3. The voter goes to the Voting machine and inserts the smart card
4. Display the election list on Voting Machine
5. The voter selects the candidate and removes the smart card
6. Print the vote as QR code and keep the smart card and paper.
7. The voter goes to the ballot box machine
8. Scan QR code and submit the paper in the machine too
9. The voter returns smart card to EGO. Then, EGO inserts the smart card on the PC and sends the completeness of the vote to the server. (Encrypted voter’s id)
10. Initialize the Smart card.

EGO = Election Gov. Officer, EGB = Election Gov. Body

Korean e-Voting model (Offline)



Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results

Election Procedure

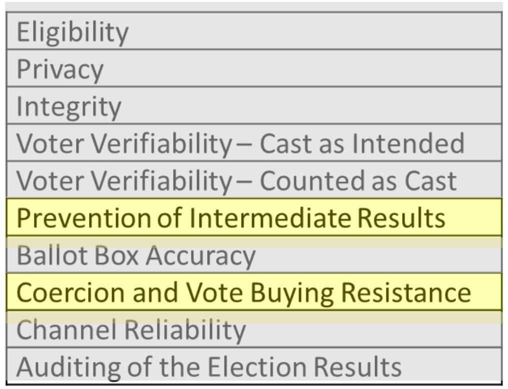
1. The voter enters to the polling station, Shows his/her identification card
2. Election Government Officer(EGO) checks the validity, If it’s valid, give the smart card to the Voter
3. The voter goes to the Voting machine and inserts the smart card
4. Display the election list on Voting Machine
5. The voter selects the candidate and removes the smart card
6. Print the vote as QR code and keep the smart card and paper.
7. The voter goes to the ballot box machine
8. Scan QR code and submit the paper in the machine too
9. The voter returns smart card to EGO. Then, EGO inserts the smart card on the PC and sends the completeness of the vote to the server. (Encrypted voter’s id)
10. Initialize the Smart card.

Nobody knows who the voter is insider polling station.

QR code is not recognizable by humans.

EGO = Election Gov. Officer, EGB = Election Gov. Body

Korean e-Voting model (Offline)



Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results

Election Procedure

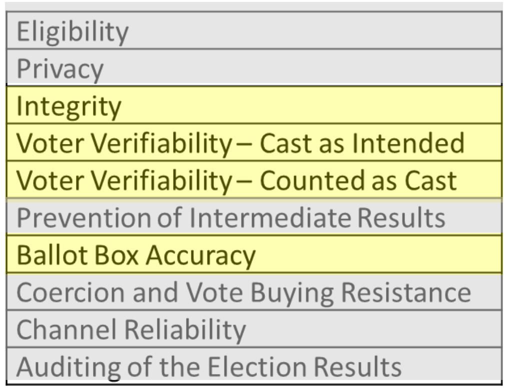
1. The voter enters to the polling station, Shows his/her identification card
2. Election Government Officer(EGO) checks the validity, If it's valid, give the smart card to the Voter
3. The voter goes to the Voting machine and inserts the smart card
4. Display the election list on Voting Machine
5. The voter selects the candidate and removes the smart card
6. Print the vote as QR code and keep the smart card and paper**.**
7. The voter goes to the ballot box machine
8. **Scan QR code and submit the paper in the machine too**

9. The voter returns smart card to EGO. Then, EGO inserts the smart card on the PC and sends the completeness of the vote to the server. (Encrypted voter's id)

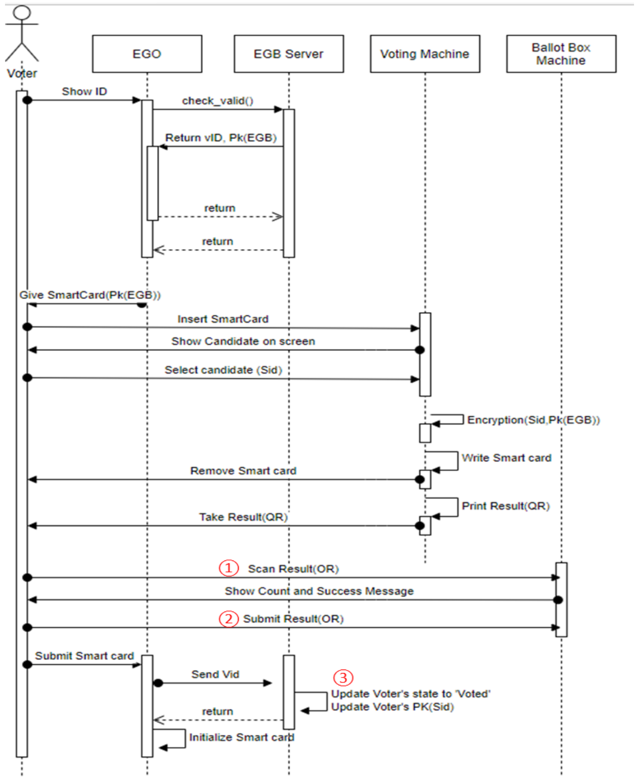
10. Initialize the Smart card.

EGO = Election Gov. Officer, EGB = Election Gov. Body

Korean e-Voting model (Offline)



Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results



In this model, there are 3 evidences to proof completeness

Correctness of tallying by e-Voting model

Audit by polling station

- Validate counts on ① Ballot Box Machine (By QR scanning) and ② Submitted paper

After the closing election, counts were announced. For safety, the vote counts are accumulated every day.

Audit by Headquarter

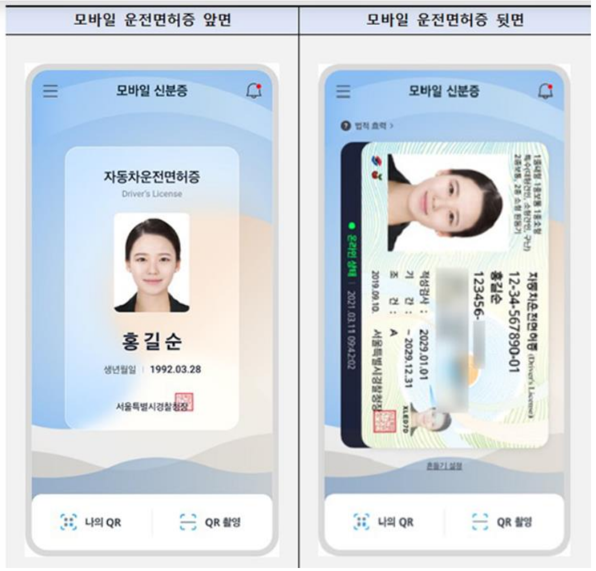
- Validate counts on ① Ballot Box Machine and ③ Counts on server

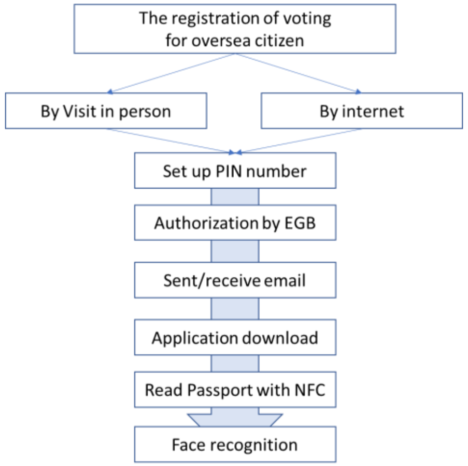
If the difference among ① . ② and ③ were found, the Election HQ verify again.

Korean e-Voting model (Online)

- Authentication

Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results





The registration of voting for oversea citizen

By Visit in person

By internet

Set up PIN number

Authorization by EGB

Sent/receive email

Application download

Read Passport with NFC

Face recognition

Why!

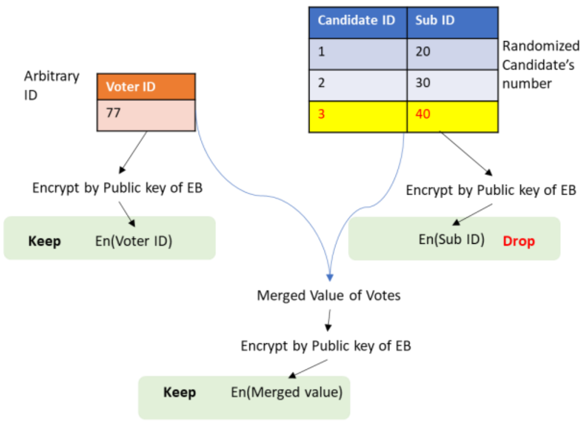
- **By historical experience:** Overseas voting was stopped in 1976.
- **Sensitive against malfunction**.

To-be model:
3 Factor authentication (What to have, What to know, Who I am)
Use Passport (a.k.a 'biometric passport') : Since 2020, the Korean gov has taken the mobile ID by NFC.
+ Pin code that voters enter when they register
+ Face recognition (Biometric measure by mobile)

Korean e-Voting model (Online)

- Eligibility
- Privacy
- Integrity
- Voter Verifiability – Cast as Intended
- Voter Verifiability – Counted as Cast
- Prevention of Intermediate Results
- Ballot Box Accuracy
- Coercion and Vote Buying Resistance
- Channel Reliability
- Auditing of the Election Results

Homomorphic Encryption(Aggregation)



Candidate ID	Sub ID
1	20
2	30
3	40

Arbitrary ID
Voter ID
77
Randomized Candidate's number
Encrypt by Public key of EB
Encrypt by Public key of EB
Keep
En(Voter ID)
En(Sub ID)
Drop
Merged Value of Votes
Encrypt by Public key of EB
Keep
En(Merged value)

Encrypted by Public Key of EGB

After casting votes,
Data is encrypted and sent to the server

To verify, the voter can receive encrypted En(Sub ID) from the server.

By Homomorphic aggregation,
The total result can't be decrypted until closing of the election.

The sum value of data is encrypted by the Public Key of the Election Government Body.
➔ This is not guaranteed to check their vote but can check whether the vote applies to the tally.
By Korean law, Vote selling, and Vote by coercion are prohibited. Then individual verification was not needed.
➔ Public official Election Act. Article 230(Corrupt Practices and Inducement by Interest),
➔ Article237(Interference with Freedom of Election)

Why!

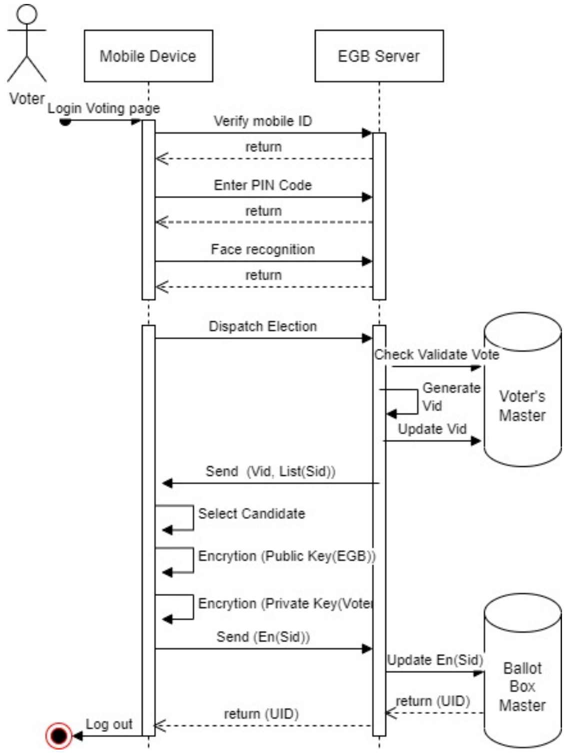
- **By Law, not allowed to trace vote individually**: for the prevention of voting by coercion and Vote Buying

By Double Envelope Encryption,
A voter's profile(=Voter ID) and vote(=Selected Candidate ID) are encrypted and kept secret.

By Homomorphic Encryption,
Decryption will happen at the end of the election. Before then, the election agency could see only the number of votes.

Korean e-Voting model (Online)

Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results



Why!

- **Should safe even if data was leaked**:

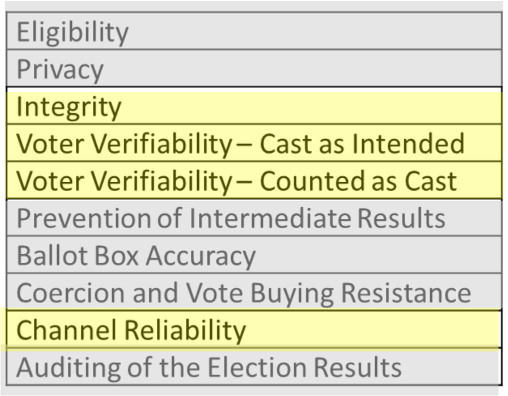
In papers of Dr.Rubin(1), Estonian i-Voting analysis(2), experts showed us servers and clients or any other system can be malfunctioned and leaked. Thus, the sepatation of data should be considered.

Separation of data

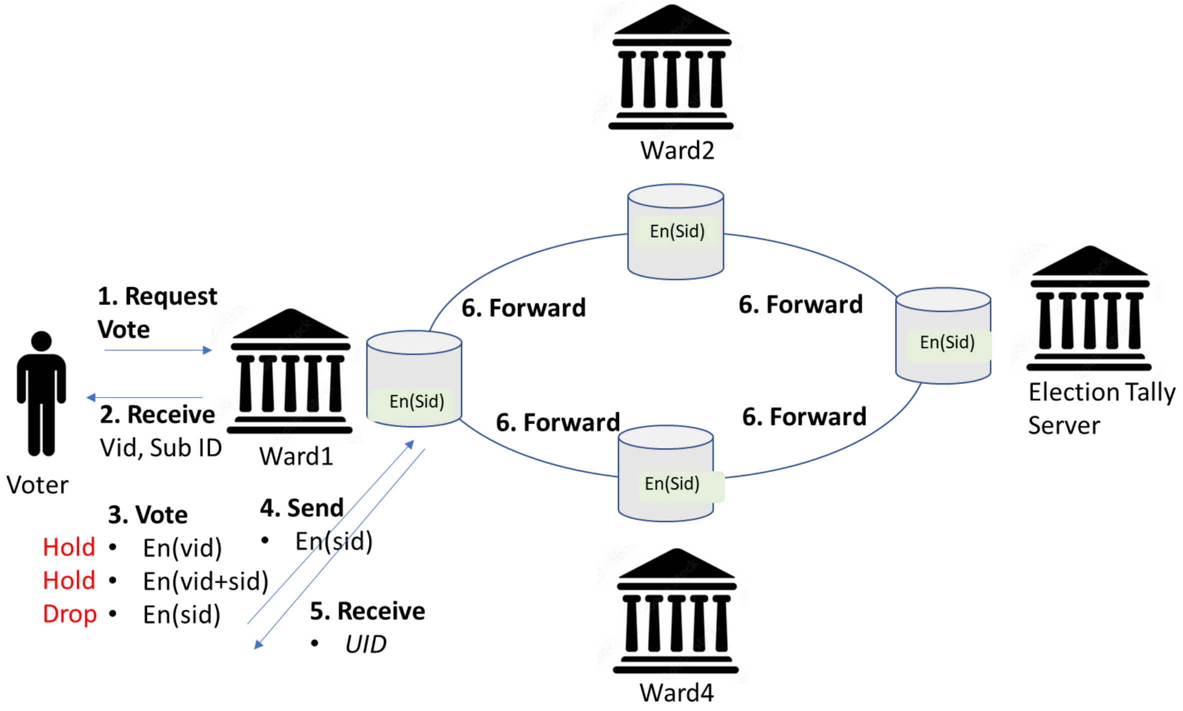
Even if vote data are leaked, they will keep secret because voters' profiles and vote results will be separated and stored in different storage.

(1) 2004. Aviel Rubin prof. (Univ of Johns Hopkins) Testimony, U.S. Election Assistance Commission
(2) 2017. Security Analysis of the Estonian Internet Voting System by Univ of Michigan, Ann arbor

Korean e-Voting model (Online)



Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results



Why!

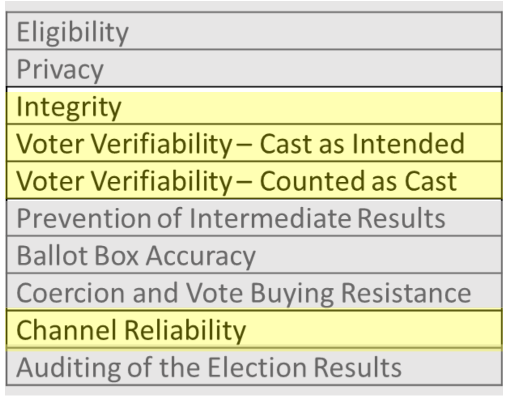
- **High Availability**:

To protect the system against DoS attacks, the election system should not be centralized.

Also..

- Support universal verification: Unique address after voting was given to the voter
- Anti-tampering
- Keep voter’s data secret: Only load “sid”(What voters select) without profile.

Korean e-Voting model (Online)



Eligibility
Privacy
Integrity
Voter Verifiability – Cast as Intended
Voter Verifiability – Counted as Cast
Prevention of Intermediate Results
Ballot Box Accuracy
Coercion and Vote Buying Resistance
Channel Reliability
Auditing of the Election Results

Goals.
– every voter can verify that their ballot was cast as intended
– every voter can verify that their ballot was collected as cast
– everyone can verify the final result on the basis of the collected ballots

Public Blockchain	Private Blockchain
Anyone access Fully decentralized Transaction is slow	Limited entities can access Partially decentralized Transaction is fast

Built-in Private blockchain for Korean e-Voting model

Thank you!

Reference

1. Morales-Rocha, Jordi Puiggali and Victor. *Remote Voting Schemes: A Comparative Analysis.* Barcelona, Spain : Scytl Secure Electronic Voting, 2007.

2. *Electronic Voting.* Solvak, Robert Krimmer · Melanie Volkamer ·Bernhard Beckert · Ralf Küsters ·Oksana Kulyk · David Duenas-Cid ·Mihkel. Bregenz, Austria : s.n., 2020. 5th International Joint Conference.

3. Jordi Barrat i Esteve, Ben Goldsmith and John Turner. *International Experience with E-Voting Norwegian E-Vote Project.* 2012.

4. González, Carlos Vegas. *The New Belgian E-voting System.* Spain : Constitutional Law eVoting Legal Lab.

5. Cytron, Lorrie Faith Cranor and Ron K. *Design and implementation of a practical security-conscious electronic polling system.* St. Louis : Washington University, 1996.

6. *E-voting and Identity.* Ammar Alkassar, Melanie Volkamer. Bochum,Germany : Springer, 2007. First International Conference, Vote-ID 2007.

7. *전자금융거래의 사용자 인증방법 평가 및 선택 가이드.* 김신영. s.l. : 금융보안원, 2015, Vol. 2015.10.

8. ULB, KU LEUVEN. *PROJET NETVOTING_BE Étude sur la possibilité d'introduire le vote Internet en Belgique.* 2020.

9. Tarrant County election security. *www.tarrantcounty.com.* [Online] Hart Verify Duo, 10 28, 2022. [Cited: 10 28, 2022.] https://www.tarrantcounty.com/en/elections/election-security.html.

10. TADAYOSHI KOHNO, ADAM STUBBLEFIELD, AVIEL D. RUBIN, DAN S. WALLACH. *Analysis of an Electronic Voting System.* Washington D.C : U.S. Election Assistance Commission, 2004.

11. Halderman†, Drew Springall† Travis Finkenauer† Zakir Durumeric† Jason Kitcat‡ Harri Hursti Margaret MacAlpine J. Alex. *Security Analysis of the Estonian Internet Voting System.* s.l. : University of Michigan, Ann Arbor, 2014.

12. Sciences, National Academy of. *Securing the Vote: Protecting American.* Washington, DC : The National Academies Press, 2018.

13. Government, US. *CYBER–SECURING THE VOTE: ENSURING THE INTEGRITY OF THE U.S. ELECTION SYSTEM.* s.l. : US Government, 2018.

14. USPS. *SECURE VOTING SYSTEM (Block Chain). US 2020/0258338 A1* USA, 8 13, 2020.

15. NIST. *Possible UOCAVA Pilot Projects for the 2012 and 2014 Federal Elections.* s.l. : the work of the UOCAVA Working Group of the Technical Guidelines Development Committee, 2011.

16. 중앙선거관리위원회. *인터넷을 활용한 재외선거인 등 신고·신청방법 도입에 관한 연구.* s.l. : 중앙선거관리위원회, 2013.

17. Piret Ehin, Mihkel Solvak, Jan Willemson,Priit Vinkel. Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly.* 2022, Vol. 39, 4.

18. Rights, Office for Democratic Institutions and Human. *ESTONIA OSCE/ODIHR Election Assessment Mission Report(PARLIAMENTARY ELECTIONS).* s.l. : Office for Democratic Institutions and Human Rights, 2011.

19. Mapped: Expats kick off French legislative elections with online voting. *https://www.france24.com/en/france/20220527-mapped-expats-kick-off-french-legislative-elections-with-online-voting.* [Online] 2022.

20. Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. *www.legifrance.gouv.fr.* [Online] France Government, July 2019. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239.

21. Souad Benmeziane, Lyes Khelladi. *i-vote : un système de vote électronique hautement sécurisé.* 2002.

22. Verified Voting Org. [Online] ES&S ExpressVote XL, 10 31, 2022. https://verifiedvoting.org/election-system/ess-expressvote-xl/.

23. Kaitlin Durbin. https://www.cleveland.com/. *Scanning problems at Cuyahoga County polling locations temporarily caused voting delays on Election Day; but 'integrity' remained intact, officials say.* [Online] www.cleveland.com, 5 3, 2022. https://www.cleveland.com/news/2022/05/scanning-problems-at-cuyahoga-county-polling-locations-causing-voting-delays-on-election-day.html.

24. Wikipedia. *Optical scan voting system.* [Online] 10 31, 2022. https://en.wikipedia.org/wiki/Optical_scan_voting_system.

25. What was the number of invalid votes caused by the resignation of Ahn Cheol-soo and Kim Dong-yeon? *The Kyunghyang Shinmun.* [Online] The Kyunghyang Shinmun, 4 27, 2022. https://www.khan.co.kr/politics/election/article/202204070600001.

26. Commission, Election Assistance. Voluntary Voting System Guidelines VVSG 2.0. *https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines.* [Online] 2 10, 2021.

27. Reform, Committee on Oversight and Government. *CYBER–SECURING THE VOTE: ENSURING THE INTEGRITY OF THE U.S. ELECTION SYSTEM.* s.l. : U.S. GOVERNMENT PUBLISHING OFFICE, 2018.

28. Safety, Ministry of the Interior and. https://www.korea.kr/. *Korean Policy Briefing.* [Online] MOIS, 9 22, 2022. https://www.korea.kr/news/visualNewsView.do?newsId=148906148.

29. 윤성현. 모바일 전자투표 연구동향 및 요구사항 분석. *한국 인터넷 정보학회.* 3 2012.

30. *재외국민선거제도에 관한 공청회 자료집.* 강경태, 박명호, 방승주, 정훈교. s.l. : Korean National Assembly , 2011. 정치개혁특별위원회 공청회.

31. *Security Standardisation Research.* Liqun Chen, Shin'ichiro Matsuo. Tokyo, Japan : Springer, 2015. Second International Conference, SSR 2015.

32. *Free or Fair Elections? The Introduction of Electronic Voting in Brazil.* SCHNEIDER, RODRIGO. 2020, Brookings Institution Press.

33. ULB, KU LEUVEN. *PROJECT NETVOTING_BE Etude sur la possibilité d'introduire le vote Internet en Belgique.* 2021.

34. Sven Heiberg and Jan Willemson, Ulikooli. *Verifiable Internet Voting in Estonia.* Tartu, Estonia : s.n.