E-voting: dream or nightmare?

Wouter Bokslag & Manon de Vries

April 29, 2015
Table of contents

1. Introduction

2. Case studies
   - Estonia
   - The Netherlands

3. Future improvements
   - Procedural
   - Technical
   - Example: Helios

4. Conclusions
Definition

E-voting: voting on, or with help of, electronic devices

I-voting: voting over the internet
Requirements

Ideal situation

- Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements
End-to-end verifiability

In the ideal case, an E-voting solution has the following properties:

- Voter can check if vote represents his choice
- Voter can check if all votes were counted properly

This is commonly referred to as *end-to-end verifiability*
Risks and benefits

Paper voting

How would you hack paper voting?
Risks and benefits

Paper voting

How would you hack paper voting?

- Counting "errors"
Risks and benefits

Paper voting

How would you hack paper voting?

- Counting "errors"
- Voting by proxy ("volmacht")
Risks and benefits

Paper voting

How would you hack paper voting?

- Counting "errors"
- Voting by proxy ("volmacht")
- Buying votes using a single blank ballot
Risks and benefits

Benefits of e-voting.

- Fast counting
- Less labor-intensive
- Cheaper?

Additional benefits of i-voting.

- No need to go to polling station
- Less voting by proxy
- Possible to vote from abroad
Risks and benefits

Drawbacks of e-voting:
- Scalability of attacks.
- Voting process is not clear for voter.
- Implementation of voting machines has more pitfalls: more expertise required.

Additional drawbacks of i-voting:
- Usage on an untrusted and unmanaged client system.
- Sending votes over an unreliable channel.
- Coercion resistance very difficult.
Case study: Estonia
Estonia

- Pioneer in I-voting
- Introduced I-voting in 2005
- Increasingly popular: 30.5% of votes are I-votes in 2015
- Uses a digital analog of ‘double envelope’ ballots
Estonia: The voting process

- National ID equipped with chip
- Stores cryptographic keys
  - used for legally binding signatures
Estonia
The voting process

Figure: Voting client / election server protocol
Estonia

The verification app

![Diagram of verification app and election server protocol](image)

**Figure**: Verification app / election server protocol
Estonia

The backend

Figure: Voting client / election server protocol

Diagram:

Storage Server

\[ B \leftarrow \{\} \]
For each vote \( v \):
\[ (b, \sigma) \leftarrow v \]
\[ \text{Verify}_{PK_{\text{voter}}}(b, \sigma) \]
\[ B \leftarrow B \cup \{b\} \]
\[ B \]

Counting Server

For each \( c \in C \):
\[ \text{counts}[c] \leftarrow 0 \]
For each \( b \in B \):
\[ c \leftarrow \text{Dec}_{SK_{\text{election}}}(b) \]
\[ \text{counts}[c] \leftarrow \text{counts}[c] + 1 \]
Output \( \text{counts} \)
Estonia

Infrastructure overview

Figure: Estonian I-voting infrastructure
Estonia

Procedures

- Large amount of (public) procedures
  - Some scenarios not handled, some poorly specified
  - Some procedures were not followed consistently
  - Some procedures were added only during the voting period
Estonia

Procedures

- System install/maintenance recorded and published on Youtube
  - Good idea: voters can verify (part of) the actions of installation, configuration and maintenance
  - Not complete though..
  - Leakage of sensitive information
Estonia

Procedures

Figure: Keyboard filmed when typing in root password
Estonia

Procedures

Figure: WiFi password readable on a written note on the wall.
Estonia

Procedures

Figure: Insecure build machine for voting application
Estonia

Attacks

- Target voter’s computer and/or smartphone
  - Malware, trigger 30 minutes after vote to circumvent vote validation
- Target counting server
  - Infect before delivery, through build server, or malicious insider
- Malicious election staff members
  - Procedures are in place to mitigate the risks, but often incomplete or not consistently enforced/followed.
Estonia

Design flaws

- No end-to-end verifiability
- Limited protection against coercion: inherent to I-voting
- 'Trust issues'
  - Trusts voter’s computer and/or smartphone
  - Trusts counting server
  - Trusts election staff
Requirements

Estonia

- Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- X Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- X Transparency/Integrity
- ✓ Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- X Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- X  Transparency/Integrity
- ✓  Ballot secrecy/privacy
- ✓  Uniqueness
- ✓  Voter eligibility
- ✓  Verifiability/auditing
- ✓  Accessibility
- ✓  Vote freedom / coercion resistance
- ✓  Availability
Requirements

Estonia

- X Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- X Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- X Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- X Verifiability/auditing
- ✓ Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- X  Transparency/Integrity
- ✔  Ballot secrecy/privacy
- ✔  Uniqueness
- ✔  Voter eligibility
- X  Verifiability/auditing
- ✔  Accessibility
- X  Vote freedom / coercion resistance
- Availability
Requirements

Estonia

- ❌ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- ❌ Verifiability/auditing
- ✓ Accessibility
- ❌ Vote freedom / coercion resistance
- ❌ Availability
Case study: the Netherlands
Netherlands: e-voting

History

- E-voting legally possible since 1965\(^1\)
  - Machines have to be certified for secrecy and usability
  - Voter should be able to correct mistakes
  - Additional requirements by lower legislation\(^2\)
- Voting machines first use in 1966
- Responsibility and choice of municipalities
- Machines may be bought or rented

\(^1\)art. 32-34 Chapter J of the Voting law (Kieswet), retracted in 2009
\(^2\)Algemene maatregel van bestuur
Netherlands: e-voting
Situation 2006

- 99% of municipalities use voting machines
- 90% Nedap, 10%SDU
Netherlands: e-voting
Netherlands: e-voting

Situation 2008

- "Wij vertrouwen stemmachines niet" group
- Prove technical vulnerabilities Nedap machine
- Fraud case with voting machines
- E-voting is stopped immediately
- Two committees are formed
- Laws are retracted, machines decertified

3 Translated: "We don't trust voting machines"
Netherlands: e-voting

Technical problems Nedap machines

- Radio signal emissions: screen signals reveal user vote
- Physical security: same key for every machine, very easy to pick locks, no seals on hardware
- Maintenance mode with password “geheim”\(^4\)
- Ability to install other software (no signature checking)

\(^4\) Translated: ”secret”
Netherlands: e-voting

Technical problems Nedap machines

After reading the results:

“[...] And with regard to the claim that our machine can play chess: I’d like to see that demonstrated”

- Jan Groenendaal, Nedap
Netherlands: e-voting

Technical problems Nedap machines

After reading the results:

“[…] And with regard to the claim that our machine can play chess: I’d like to see that demonstrated”

- Jan Groenendaal, Nedap
Requirements

Dutch e-voting

- Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements
Dutch e-voting

- X Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch e-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements
Dutch e-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements
Dutch e-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✔ Uniqueness
- ✔ Voter eligibility
- ✔ Verifiability/auditing
- ✔ Accessibility
- ✔ Vote freedom / coercion resistance
- ✔ Availability
### Requirements

**Dutch e-voting**

- **X** Transparency/Integrity
- **X** Ballot secrecy/privacy
- **✓** Uniqueness
- **✓** Voter eligibility
- **X** Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch e-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- X Verifiability/auditing
- ? Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch e-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- X Verifiability/auditing
- ? Accessibility
- X Vote freedom / coercion resistance
- Availability
Requirements

Dutch e-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- X Verifiability/auditing
- ? Accessibility
- X Vote freedom / coercion resistance
- ? Availability
Netherlands: i-voting

- Multiple experiments in 2004 and 2006
- KOA (kiezen op afstand) and RIES: Rijnland Internet Election System
- 4,835 (KOA: EU 2004)
- 120,000 (RIES: water boards 2004)
- 19,815 (RIES: parliament 2006)
- Canceled after 3 separate studies in 2008
Netherlands: i-voting

RIES

- RIES: Rijnland Internet Election System
- Developed for Water Board (Waterschappen) elections in 2004
- 72,235 (Rijnland), 50,196 (De Bommel)
- First experiment for normal elections in 2006
- Aimed at citizens living abroad
- 19,815 voters 2006
- "End-to-end verifiability"
Netherlands: i-voting

RIES

- Researched by Gonggrijp et al, TUE and Fox-IT
- Cryptographic flaws
  - DES and 2DES
  - Valid vote codes can be generated
- Assumes users PC is safe
Netherlands: i-voting

RIES

Cryptographic flaws:

- \( K_{voter} = 2\text{DES}_{K_{genvoterkey}}(m) \)
  - Generated before the election for each eligible voter
- Always the same \( K_{genvoterkey} \)
- Encrypted vote = \( MDC(\text{DES}_{K_{voter}}(\text{choice}, ELID, yearOfBirth)) \)

- When an attackers breaks \( K_{genvoterkey} \) he can:
  - Determine who was eligible to vote in election
  - If (s)he voted
  - Who (s)he voted for
Netherlands: i-voting

RIES

Technical flaws:

- XSS
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; –)
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; –)
- Predictable random tokens (depends on time as seed)
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (` OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (’ OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (’ OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
- Voting station can see canceled votes
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
- Voting station can see canceled votes
- Old apache and MySQL version with known vulnerabilities
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
- Voting station can see canceled votes
- Old apache and MySQL version with known vulnerabilities
- Voting codes in browser history
Netherlands: i-voting
RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; --)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
- Voting station can see canceled votes
- Old apache and MySQL version with known vulnerabilities
- Voting codes in browser history
- DoS possible with ';' in URL
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
- Voting station can see canceled votes
- Old apache and MySQL version with known vulnerabilities
- Voting codes in browser history
- DoS possible with ’;’ in URL
- Usage of SSL 2.0 possible
Netherlands: i-voting

RIES

Technical flaws:

- XSS
- SQL injection (' OR 1=1; –)
- Predictable random tokens (depends on time as seed)
- Exceptions are not handled, just logged
- Testing code mixed with production code (hardcoded salt)
- Voting station can see canceled votes
- Old apache and MySQL version with known vulnerabilities
- Voting codes in browser history
- DoS possible with ‘;’ in URL
- Usage of SSL 2.0 possible
- Access to server folders and maintenance windows
Netherlands: i-voting
RIES

<table>
<thead>
<tr>
<th>RIES Operationeel Beheer Server &quot;ss1&quot;</th>
<th>Server &quot;ss1&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operationeel</td>
<td>Home</td>
</tr>
</tbody>
</table>

**Overzicht verkiezingen**

Hieronder zie je een overzicht van alle verkiezingen en hun status.

<table>
<thead>
<tr>
<th>lå</th>
<th>Alias</th>
<th>status</th>
<th>naam</th>
<th>start</th>
<th>stop</th>
<th>delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>9999</td>
<td>Testverkiezing</td>
<td>opr</td>
<td>Testverkiezing 2008</td>
<td>2007-12-10 12:00:00</td>
<td>2007-12-10 12:00:00</td>
<td>6</td>
</tr>
<tr>
<td>3330</td>
<td>nlg2</td>
<td>opr</td>
<td>Hoogheemraadschap Schelde en de Krimpenerwaard</td>
<td>2007-12-01 12:00:00</td>
<td>2007-12-01 12:00:00</td>
<td>4</td>
</tr>
<tr>
<td>0101</td>
<td>vltzesta</td>
<td>closed</td>
<td>Verkz PRB72,PCO</td>
<td>2008-06-09 17:46:00</td>
<td>2008-06-09 22:00:00</td>
<td>2</td>
</tr>
<tr>
<td>8001</td>
<td>nl</td>
<td>finished</td>
<td>Hoogheemraadschap van Rijnland</td>
<td>2008-06-16 12:00:00</td>
<td>2008-06-16 12:00:00</td>
<td>5</td>
</tr>
<tr>
<td>7201</td>
<td>nl</td>
<td>opr</td>
<td>Waterschap Riekerland</td>
<td>2008-06-24 12:00:00</td>
<td>2008-06-24 12:00:00</td>
<td>5</td>
</tr>
</tbody>
</table>
Requirements
Dutch i-voting

- Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch i-voting

- X Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements
Dutch i-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements
Dutch i-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch i-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- X Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch i-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- X Voter eligibility
- X Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch i-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✓ Uniqueness
- X Voter eligibility
- X Verifiability/auditing
- X Accessibility
- Vote freedom / coercion resistance
- Availability
Requirements

Dutch i-voting

- X Transparency/Integrity
- X Ballot secrecy/privacy
- ✔ Uniqueness
- X Voter eligibility
- X Verifiability/auditing
- X Accessibility
- X Vote freedom / coercion resistance
- Availability
## Requirements

**Dutch i-voting**

- **X** Transparency/Integrity
- **X** Ballot secrecy/privacy
- ✓ Uniqueness
- **X** Voter eligibility
- **X** Verifiability/auditing
- **X** Accessibility
- **X** Vote freedom / coercion resistance
- **X** Availability
Netherlands: e-voting

Situation now

2013: Research “every vote counts”

- Every voter should be able to understand and verify the voting process
- 4 scenario’s: 3 e-voting + paper voting
- Voting with electronic printer plus scanner best scenario
- Technical, functional and security requirements for e-voting
- Independent certification organization
- Central organization and responsibility
- Planning: 2018/2019
2015: new plans for e-voting using printers and scanners
Future improvements
Clear requirements

Not only requirements for accessibility, but also procedural and technical requirements
We (...) strongly believe that trade secrets, secret computer programs and secret test reports have absolutely no place in any democratic election.

-Gonggrijp et al. 2006
Comprehensive procedures

Procedures for certification, maintenance, for setting up systems and dismantling.

Clear procedures about sanctions:
- When is an electronic election canceled?
- What happens if requirements are not met?

Clear procedures about updating machines and techniques
Auditing and verifiability

Independent certifying and auditing body
Security by design

Security by design, made with state actors as threat model
Possible interesting techniques for e-voting
Homomorphic encryption

- Homomorphic encryption allows computations to be carried out on cipher text

\[ \mathcal{E}(a) + \mathcal{E}(b) = \mathcal{E}(a + b) \]

- Can decrypt \( \mathcal{E}(a + b) \) to obtain \( a + b \) without knowledge of \( a \) or \( b \)

- Ideal feature for E-voting: count votes without knowing any individual vote.
Homomorphic encryption

- In the ElGamal cryptosystem, we have public key $h = g^x$ with secret key $x$. The encryption function is $E(m) = (g^r, m \cdot h^r)$ with random $r$. The homomorphic property is:

$$E(g^{m_1}) \cdot E(g^{m_2})$$

$$= (g^{r_1}, g^{m_1} \cdot h^{r_1})(g^{r_2}, g^{m_2} \cdot h^{r_2})$$

$$= g^{r_1+r_2}, g^{m_1+m_2} \cdot h^{r_1+r_2}$$

$$= E(g^{m_1+m_2})$$

- Decryption would yield $g^{m_1+m_2}$, so we have to solve DL problem. Feasible due to small solution space.
Multi-party decryption and secret sharing

- Idea: share a secret among multiple parties, that have to work together to reconstruct and use the secret
- Algorithm: Shamir’s Secret Sharing

Figure: A second-degree polynomial is uniquely defined by three points.

- Need at least \( \text{degree} + 1 \) shares to obtain secret.
- To be used in finite field.
Example: Helios

- Helios is an open-source I-voting solution
- Also offers voting services through their website
- Suitable for low-coercion elections
  - Limitation inherent to I-voting
- End-to-end verifiability:
  - Any voter can check if his vote was taken into account
  - Any voter can check if the votes were counted properly
Example: Helios

- Alice selects the election
- Ballot Preparation System leads Alice through the ballot questions and records her answers
- After confirmation, vote is encrypted and commitment hash is generated
- Alice can now choose to audit or seal the encrypted vote
  - Audit: Decrypt vote, check if vote indeed represents her choices
  - Seal: Identity is checked, all plaintext data deleted, vote is registered by Helios.
- Alice may cast a new vote at any time, invalidating her previous vote
Example: Helios

Counting

- When the election period is over, voting is disabled
- Encrypted votes are counted using exponential ElGamal and multi-party decryption.
- All encrypted votes are publicly accessible on bulletin board, either named or anonymously
  - This allows anyone to verify if his vote was indeed taken into account, and to verify if vote counting was done properly.
Example: Helios

- Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- ✓ Verifiability/auditing
- Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- ✓ Verifiability/auditing
- ✓ Accessibility
- Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- ✓ Verifiability/auditing
- ✓ Accessibility
- X Vote freedom / coercion resistance
- Availability
Example: Helios

- ✓ Transparency/Integrity
- ✓ Ballot secrecy/privacy
- ✓ Uniqueness
- ✓ Voter eligibility
- ✓ Verifiability/auditing
- ✓ Accessibility
- X Vote freedom / coercion resistance
- ✓ Availability
Final conclusions
## Overview requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Helios</th>
<th>Estonia</th>
<th>E-voting NL</th>
<th>I-voting NL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency/ integrity</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ballot secrecy/ privacy</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Voter eligibility</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Verifiability/ auditing</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Accessibility</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>X</td>
</tr>
<tr>
<td>Vote freedom/ coercion resistance</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Availability</td>
<td>✓</td>
<td>X</td>
<td>?</td>
<td>X</td>
</tr>
</tbody>
</table>
Opinion

- E-voting and I-voting are pretty *hot topics* nowadays
- However, the risks are significant
- Reliable E-voting solutions are a possibility, if sufficient effort is put into designing a verifiable, open system
  - However, not certain the risks are worth the gain
- I-voting, in our opinion, is fundamentally problematic and should not be considered for high-stakes elections without further breakthroughs.
# Bibliography

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. Adida</td>
<td>Helios: Web-based Open-Audit Voting</td>
</tr>
<tr>
<td>D. Springall et al.</td>
<td>Security Analysis of Estonia’s Internet Voting System</td>
</tr>
<tr>
<td>R. Gongrijp</td>
<td>It was a bad idea anyway</td>
</tr>
<tr>
<td>R. Gongrijp et al.</td>
<td>Nedap / Groenendaal ES3B voting computer</td>
</tr>
<tr>
<td>R. Gongrijp et al.</td>
<td>RIES - Rijnland Internet Election System: A Cursory Study of Published Source Code</td>
</tr>
<tr>
<td>Fox IT</td>
<td>Advisering toelaatbaarheid internetstemvoorziening waterschappen</td>
</tr>
<tr>
<td>Adviescommissie inrichting verkiezingsproces</td>
<td>Stemmen met vertrouwen</td>
</tr>
<tr>
<td>R. Verbij</td>
<td>Dutch E-Voting opportunities</td>
</tr>
<tr>
<td>Commissie onderzoek elektronisch stemmen in het stemlokaal</td>
<td>Elke stem telt</td>
</tr>
</tbody>
</table>
Questions?