Assuring Trust, Privacy and Integrity for Internet Voting

Ed Gerck, Ph.D.
CEO and VP of Technology, Safevote, Inc., San Rafael, California, US
Chairman of the Board, IVTA, Washington, D.C.

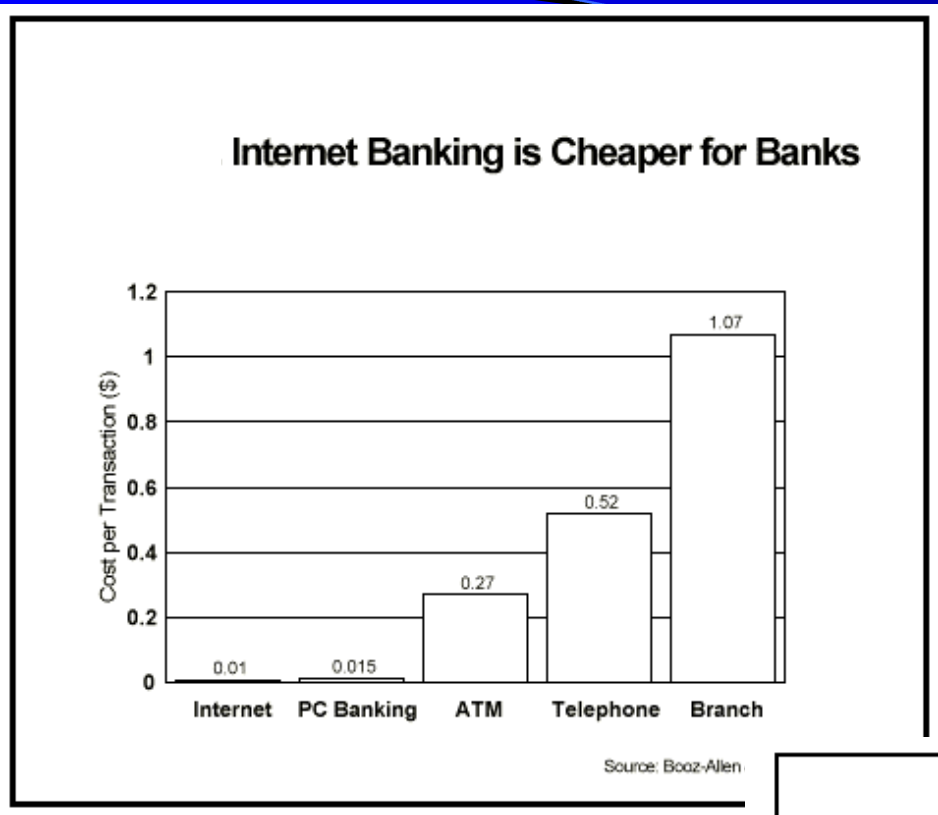
International Conference on E-Government for Development
10-11 April, 2002. Palazzo dei Normanni, Palermo, Italy.

SAFEVOTE℠

The Internet Voting Technology Alliance is a open forum on Internet voting technology

- Safevote is a co-founder of the IVTA – http://www.ivta.org
- The Internet Voting Technology Alliance includes:
  - Companies
  - Universities, private and public research centers
  - Individuals
  - Government sectors
- The IVTA is an Internet standards setting body specific for voting applications, including public elections, that:
  - Offers open participation
  - Provides for unification of standards without integration
  - Uses peer public review procedures with public workgroups
  - Provides protocol certification according to IVTA standards
  - Is non-profit
  - Is not a vendor association

Cost comparisons for other types of transaction clearly favor the Internet.



Cost to Process Airline Tickets

$8.00: Travel agent books, using computer reservation system
$6.00: Travel agent books direct with airline
$1.00: Customer books "electronic ticket" direct with airline

Source: Air Transport Association of America, 11/20/97

SAFEVOTE℠

In public elections, the cost of each vote cast should reduce 20-fold with Internet voting.

Public elections can also benefit from ICT!

- Voters already have their voting equipment (PCs at home or in the office)
- Voters already know how to use their voting equipment
- The state needs to invest less in public voting equipment and personnel
- Average cost per vote cast using current methods (U.S.): $3.00 to $7.00
- Estimated cost with Internet voting system: $0.20

Less investment and less operational costs

What Voters Want

This question is not about increasing voter participation!

The issue here is voter preference.

Contra Costa County, Calif., November 2000 – 307 voters polled at the precinct

Would You Use the Internet to Vote:

- 60% would vote from home
- 34% would prefer to vote from the workplace
- 5% would prefer to use the Internet to vote at precincts
- 1% did try the system even though they declared they were completely opposed to the idea of Internet voting

Note: When compared with Internet voting, mail and phone voting were not even mentioned by voters.

Fact: E-Democracy needs assurances for trust, privacy and integrity.

" On the Internet, nobody knows you're a dog."

"Denial of Service has no solution."

"Computers are never secure."

"We need paper proof."

...

SAFEVOTE℠

If we can use the Internet …

- If we can use the Internet to buy software
- If we can use the Internet for cybershopping
- If we can use the Internet for online banking
- If we can use the Internet to trade stock
- If we can use the Internet for proxy voting
- If we can use the Internet for Income Tax returns

…..

Why can't we use it for public elections?

SAFEVOTE℠

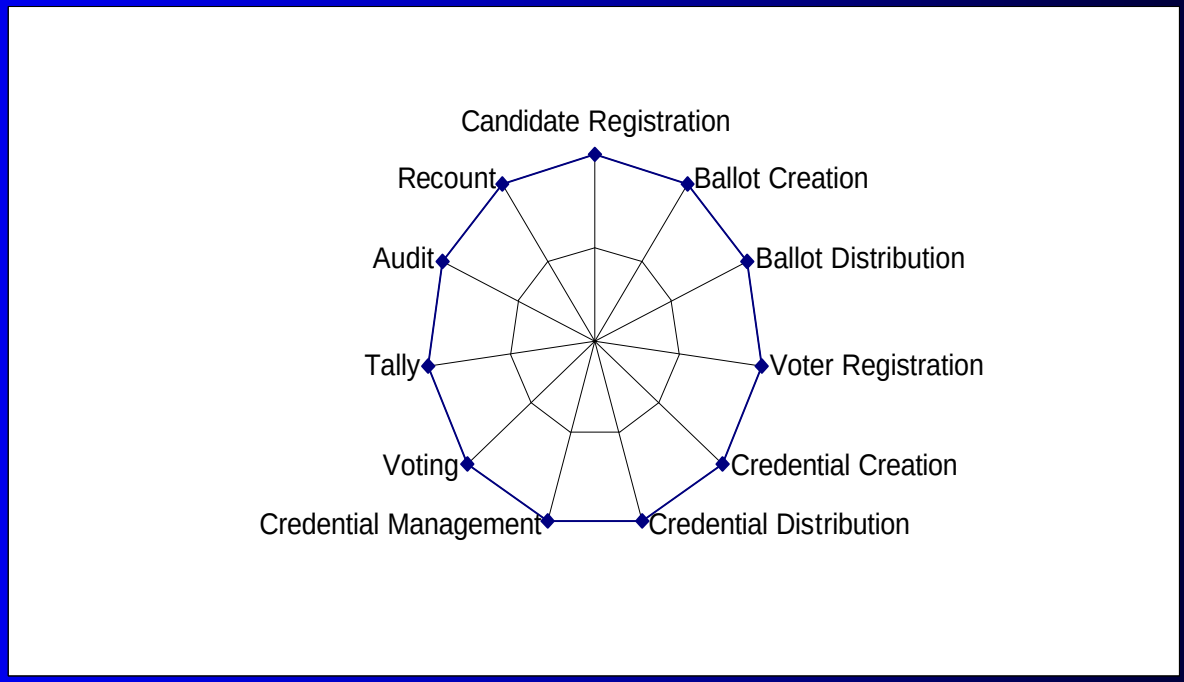
Public elections are unlike any other type of transactions. Internet voting is not the same as filling-out online forms.

- Public elections need secret votes
- Public elections need anonymous votes
- Public elections need to be correct
- Public elections need to be verifiable
- Public elections need to be honest
- Public elections need to be accessible

Not like accounting
Not like bank transactions
Not like e-commerce
Not like other e-government transactions

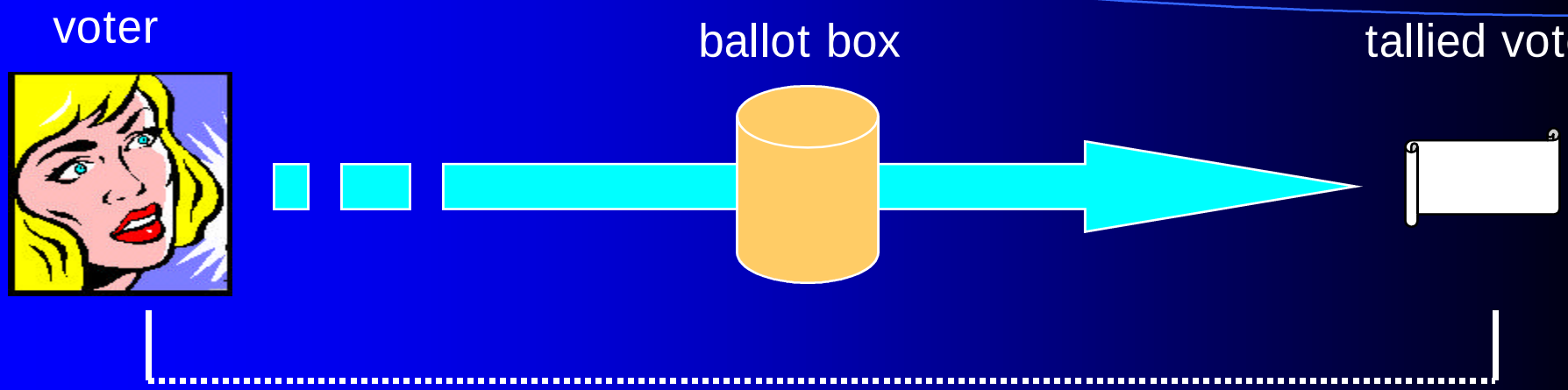
SAFEVOTE℠

An election is a open-loop process that cannot be verified as one could verify payment for a traffic fine or a book.



- No receipt: Voter receipts are NOT possible
- No outside knowledge of the transaction: the ballot is secret

The Fundamental Problem of Voting



"vote gap"

Low Reliability

The voter cannot see her tallied vote, hence the voter cannot know whether her vote will be counted as selected.

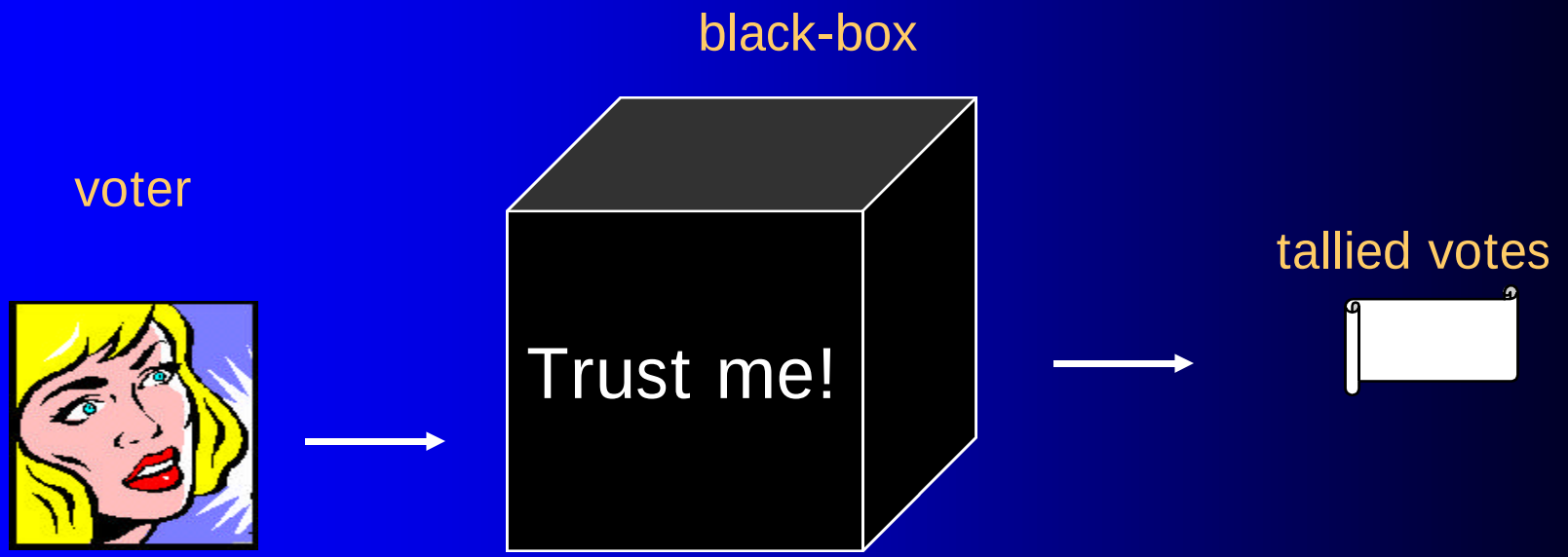
No one should be able to prove how a voter voted, not even the voter herself. And yet, society must be confident that the result is reliable.

Voters must not be linkable to votes, and vice-versa.

- I know all voters and I know all votes
- But … if I see the vote, I must not see the voter
- But … if I see the voter, I must not see the vote

HOW CAN INTEGRITY BE GUARANTEED?

One possibility: Trust Me!



Trust, Privacy and Integrity for Internet Voting cannot be provided by "trust me!"

Trust, Privacy and Integrity for Internet Voting can be provided by fulfilling a set of 16 strict performance requirements developed with the IVTA

1. ***Fail-safe voter privacy***
2. ***Collusion-free vote secrecy***
3. ***Verifiable election integrity***
4. ***Fail-safe privacy in verifiability***
5. ***Physical recounting and auditing***
6. ***100% accuracy***
7. ***Represent blank votes***
8. ***Prevent overvotes***
9. ***Provide for null ballots***
10. ***Allow undervotes***
11. ***Authenticated ballot styles***
12. ***Manifold of links –*** avoid single points of failure even if improbable
13. ***Off-line secure control structure***
14. ***Technology independent***
15. ***Authenticated user-defined presentation***
16. ***Open review, open code***

SAFEVOTE℠

Example: 1. Fail-safe voter privacy

Voter privacy is the inability to link a voter to a vote.

- Lack of voter privacy means: vote buying, voter coercion, and lack of election integrity!
- Must NOT depend on policy, computation, or even cryptography.
- Must NOT depend on election officials.
- Voter privacy is NOT anonymity.
- US: Law is powerless to break voter privacy.

  (Note: in the UK legal procedures may break voter privacy)

Counterexample: What happens if the definition of a voted ballot uses candidate names?

This is NOT in conformance and breaks voter privacy.

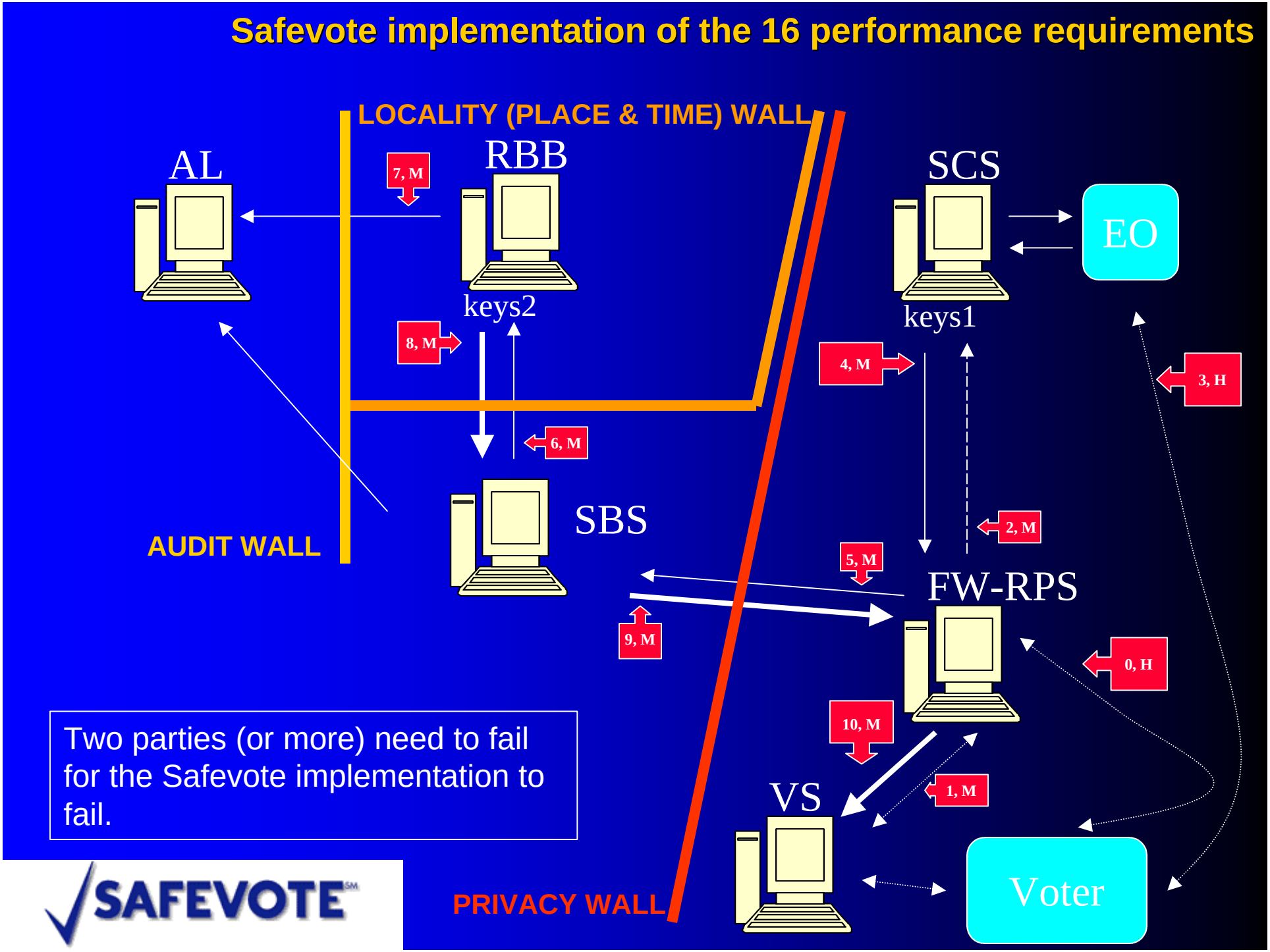
Why?

- Patterns of voted names can be, and have been, used to break voter privacy and allow voter coercion.
- It becomes difficult, if not impossible, to guarantee correctness of the tallying software (and platform).

Safevote Solution:

Use non-descriptive names for the candidates (AA, AB, UZ, …), linked randomly to each other by means of a secret key that is not revealed before and during the election, and further randomized for each vote cast, which randomization can be tested and uniquely undone for audit purposes after the election. (Safevote patent pending).

Safevote implementation of the 16 performance requirements



Two parties (or more) need to fail for the Safevote implementation to fail.

SAFEVOTE℠

Safevote has developed and tested technology for private and secure Internet voting.

- 5 years of technology development
- 2 years of commercial deployment
- 4 main products and services, for public and private sector voting
- 6 pending patents
- Highlights:
  - Provides assurances for trust, privacy and integrity
  - Real-word tested applications with excellent user feedback
  - COTS products and services delivered in the U.S., Brazil and Sweden

SAFEVOTE℠

Safevote is involved with Internet Voting projects in the private and public sectors

- California Secretary of State, US
- Contra Costa County, California, US
- Umea University Student Union, Sweden
- Umea University
- Statskontoret, Swedish Parliament, Sweden
- Aftonbladet's Ungt val 2002 project, Sweden
- Federal Voting Assistance Program, US
- Unigraphics User's Group, US
- AEITA, Brazil

SAFEVOTE℠

Summary of References

Voting System Requirements:

http://www.safevote.com/ifc01.pdf

http://www.thebell.net/papers/vote-req.pdf

Specifications, demos, test results:

http://www.safevote.com

http://www.MySafevote.com

SAFEVOTE℠

Assuring Trust, Privacy and Integrity for Internet Voting

Ed Gerck, Ph.D.
CEO and VP of Technology, Safevote, Inc., San Rafael, California, US
Chairman of the Board, IVTA, Washington, D.C.

International Conference on E-Government for Development
10-11 April, 2002. Palazzo dei Normanni, Palermo, Italy.

SAFEVOTE℠