sep 2007
Mexico

(personal) Lessons from Brazil's pioneering experience with e-Vote

Prof. Pedro A. D. Rezende

Computer Science – University of Brasília

Colaboration: Forum do Voto Seguro - CIVILIS

It's not just Voting Machines

Brazil's pioneer e-Vote experiences include(d):

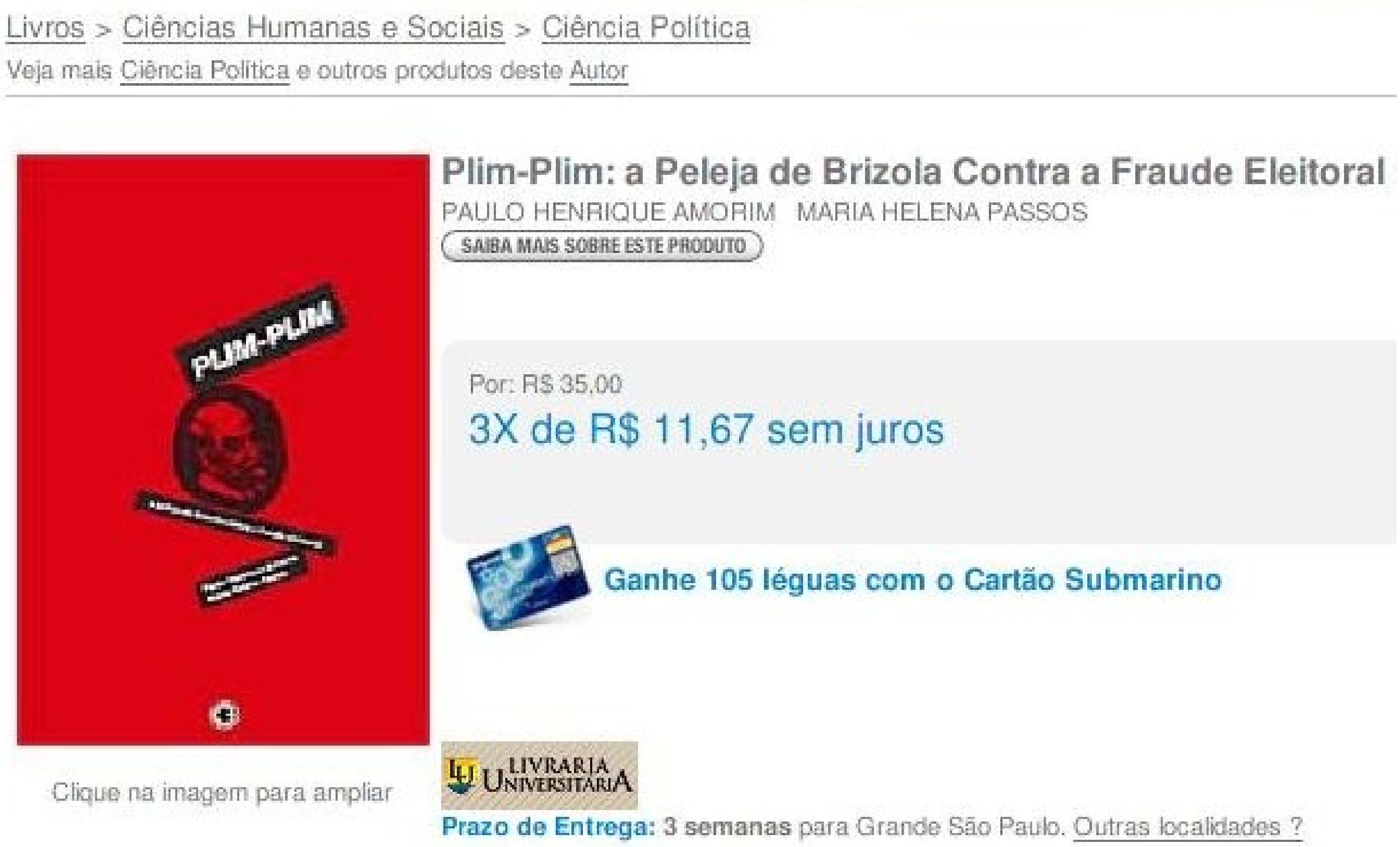
- Tallying in Rio de Janeiro state, 1982
- Voter Re-registration, 1985
- VM modeling and first procurements, 1996
- Nationwide automation, 2000.

The vote got dematerialized, but not the need for it:

1- to be cast secretly, **AND**

2- to be counted correctly.

Proconsult, 1982:
vote tallying enigma



Livros > Ciências Humanas e Sociais > Ciência Política

Veja mais Ciência Política e outros produtos deste Autor

Plim-Plim: a Peleja de Brizola Contra a Fraude Eleitoral

PAULO HENRIQUE AMORIM   MARIA HELENA PASSOS

SAIBA MAIS SOBRE ESTE PRODUTO

Por: R$ 35,00

3X de R$ 11,67 sem juros

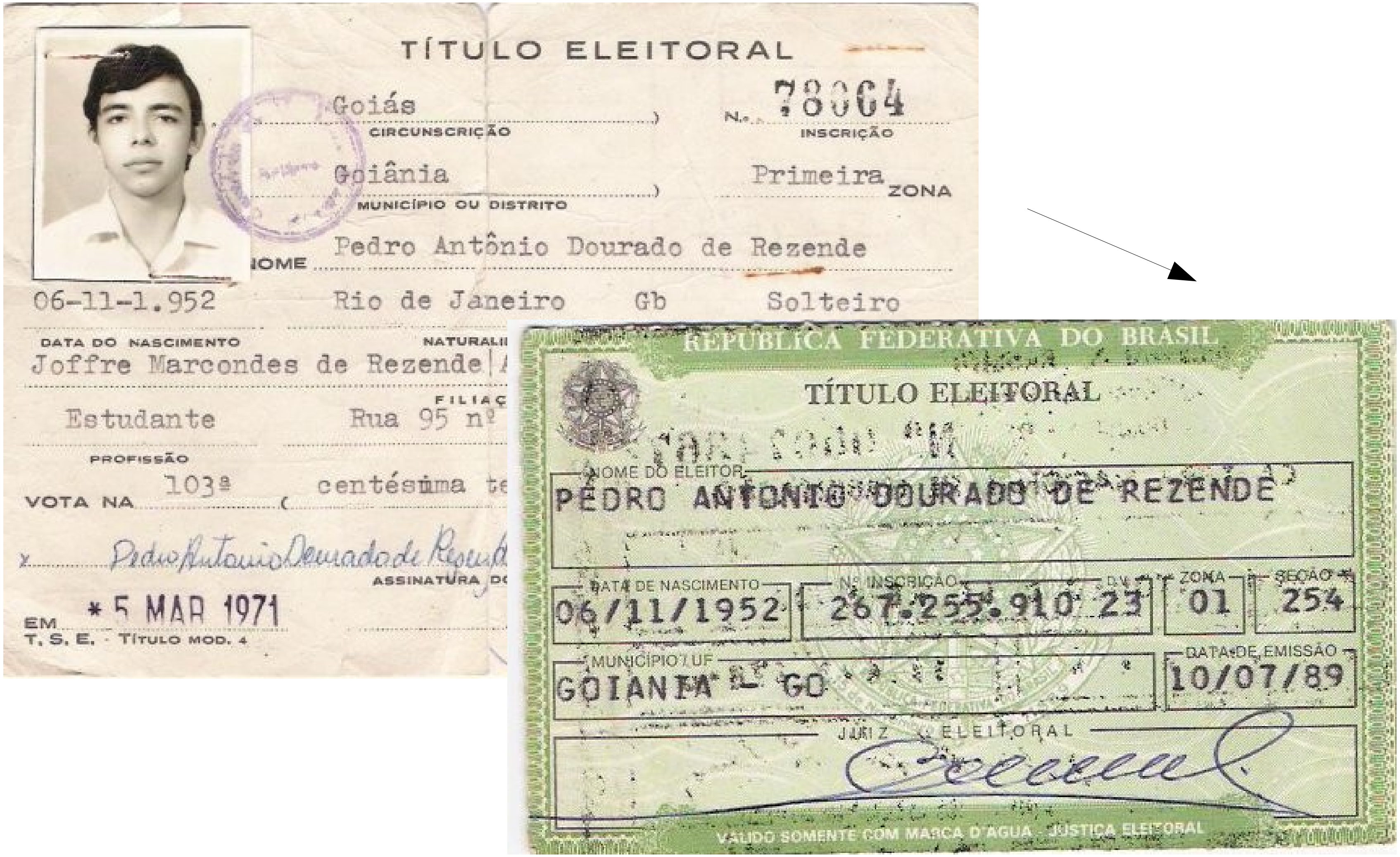
Ganhe 105 léguas com o Cartão Submarino

Clique na imagem para ampliar

LIVRARIA UNIVERSITARIA

Prazo de Entrega: 3 semanas para Grande São Paulo. Outras localidades ?

Re-registration, 1985: modernizing ...



TÍTULO ELEITORAL

Goiás
CIRCUNSCRIÇÃO

N.º 78064
INSCRIÇÃO

Goiânia
MUNICÍPIO OU DISTRITO

Primeira ZONA

NOME Pedro Antônio Dourado de Rezende

06-11-1.952
DATA DO NASCIMENTO

Rio de Janeiro Gb Solteiro
NATURALI

Joffre Marcondes de Rezende | A
FILIAÇ

Estudante
PROFISSÃO

Rua 95 nº

VOTA NA 103ª (centésima te

x Pedro Antonio Dourado de Rezende
ASSINATURA DO

EM *5 MAR 1971

T. S. E. - TÍTULO MOD. 4

REPÚBLICA FEDERATIVA DO BRASIL

TÍTULO ELEITORAL

NOME DO ELEITOR
PEDRO ANTONIO DOURADO DE REZENDE

DATA DE NASCIMENTO	Nº INSCRIÇÃO	D.V.	ZONA	SEÇÃO
06/11/1952	267.255.910	23	01	254

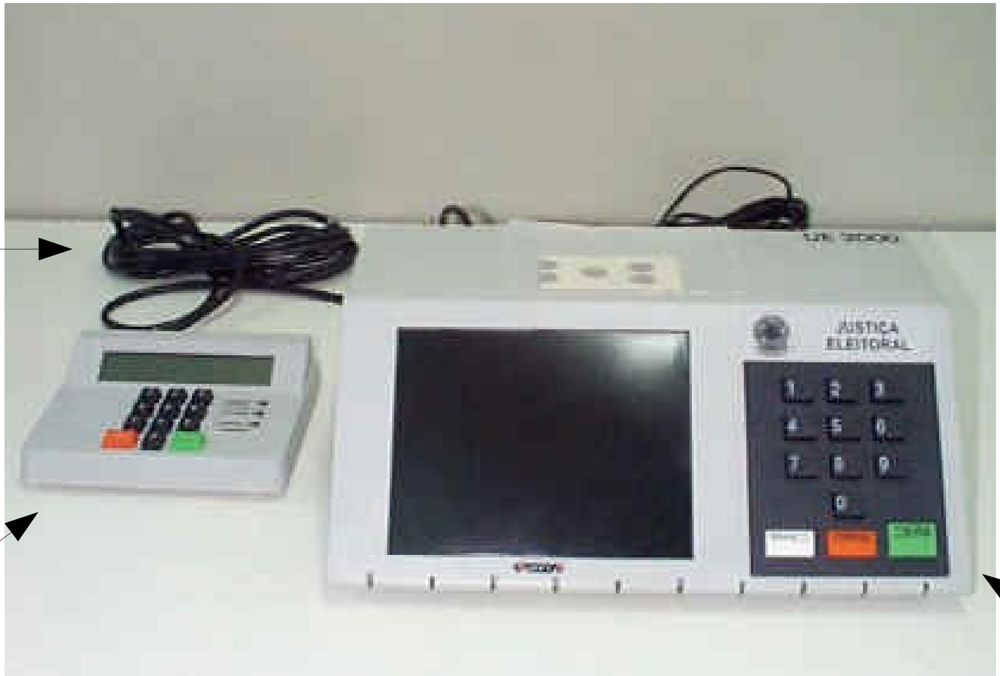
MUNICÍPIO / UF	DATA DE EMISSÃO
GOIANIA - GO	10/07/89

JUIZ ELEITORAL

VÁLIDO SOMENTE COM MARCA D'AGUA - JUSTIÇA ELEITORAL

VM model selected, 1994

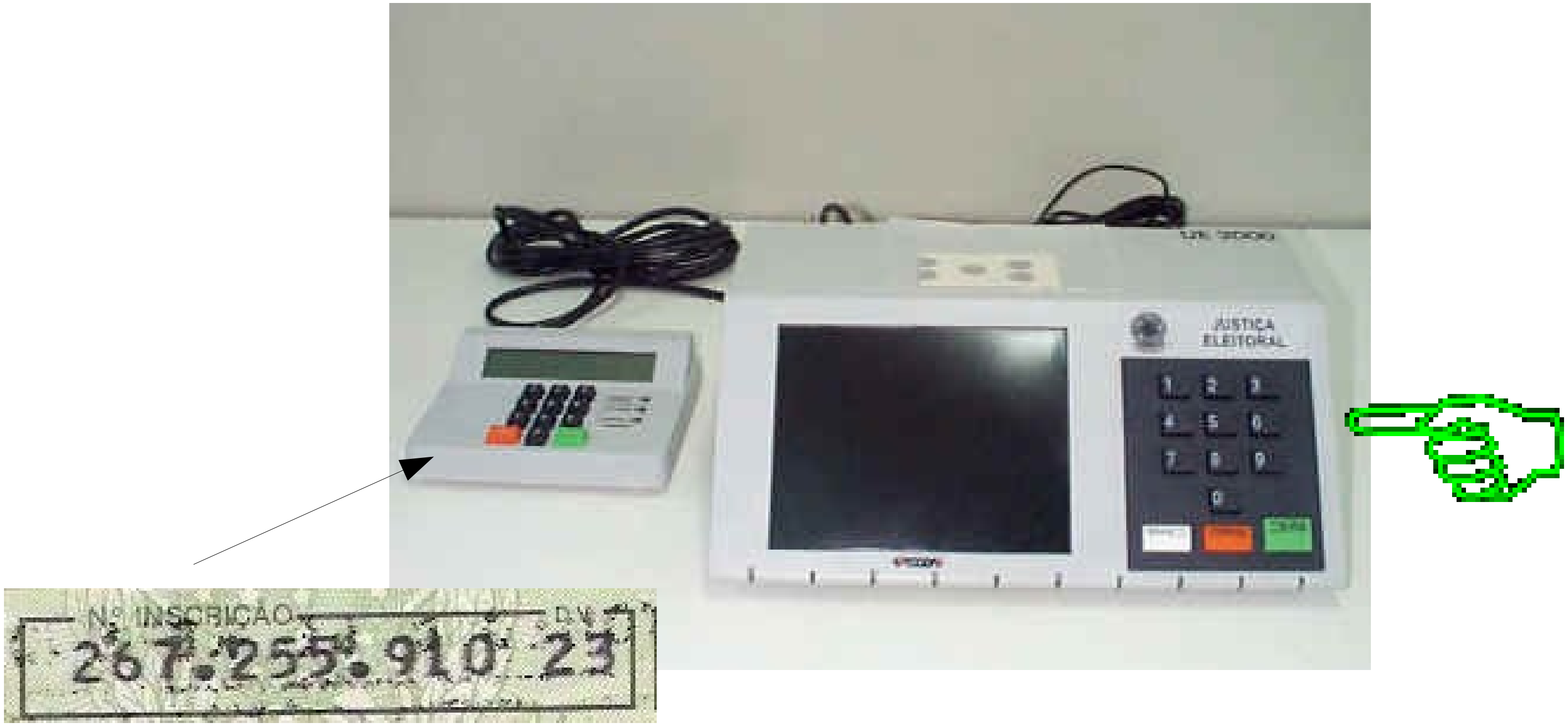
8 m. cord linking both



Voter Identification Terminal

Direct-Recording Electronic (DRE) Voting Machine

VM model selected, 1994: “umbilical” DRE



Voter Id ? Voter's vote

Self-validation

[Last link of an alleged “*Thorough, verifiable chain of custody*”]

How it can be turned off and say “OK” regardless:

[**gray**: file setup.bat, VM model 2000; **blue**: trojan horse]

```
....
diskfix c: /vs > nul
REM if errorlevel 1 goto TentaRecuperar
ckpack c:\raiz.crc c:\ > nul
REM if errorlevel 1 goto ebatger
....
```

Analysis published at Brazil's Media Observatory, sep 7, 2004

http://observatorio.ultimosegundo.ig.com.br/artigos.asp?cod=293ENO002

With self-validation off...

Simple code can, say, transfer 5% of votes from candidate A (“13”) to candidate B (“45”)

[code in C language, hypothetical names for data structures]

```
int ratio = 40;
int x = br.governor.votes[“13”]/ratio;
br.governor.votes[“45”] += x;
br.governor.votes[“13”] -= x;
self_erase_this_trojan();
```

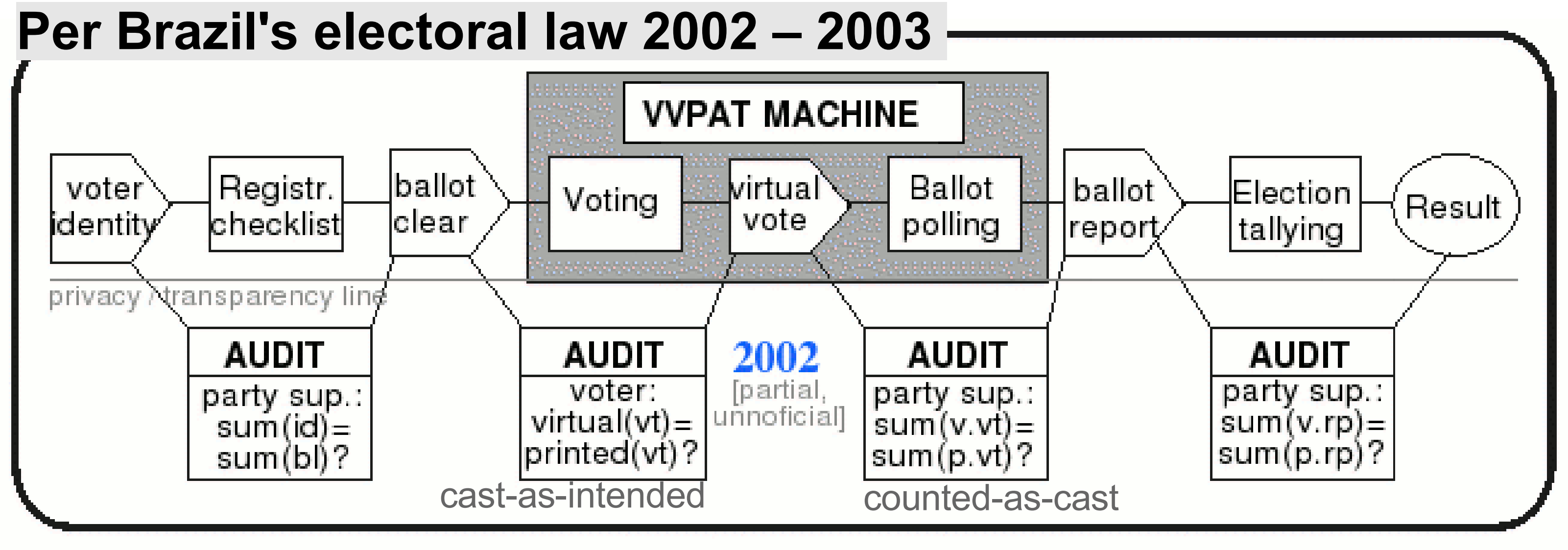
upon interception of final recording of ballot report, before encryption. http://www.cic.unb.br/docentes/pedro/trabs/SVE.htm

“Security”

Technical concept: **Security = Protection Control**

- *To Protect* is **NOT** transitive nor intransitive, it is a bi-transitive verb.
- One Protects **SOMEONE** (with some interest) **FROM SOMETHING** (some risk), **NOT** “*the system*”
- Systems fielding more than 2 interests yield risks of type **COLUSION.** In this case, security becomes a **balancing act** between risks and duties amongst interested parties (secrecy vs. transparency)

Evolution of a model



Per Brazil's electoral law 2002 – 2003

VVPAT MACHINE

voter identity

Registr. checklist

ballot clear

Voting

virtual vote

Ballot polling

ballot report

Election tallying

Result

privacy / transparency line

AUDIT
party sup.: sum(id)= sum(bl)?

AUDIT
voter: virtual(vt)= printed(vt)?

2002
[partial, unnoficial]

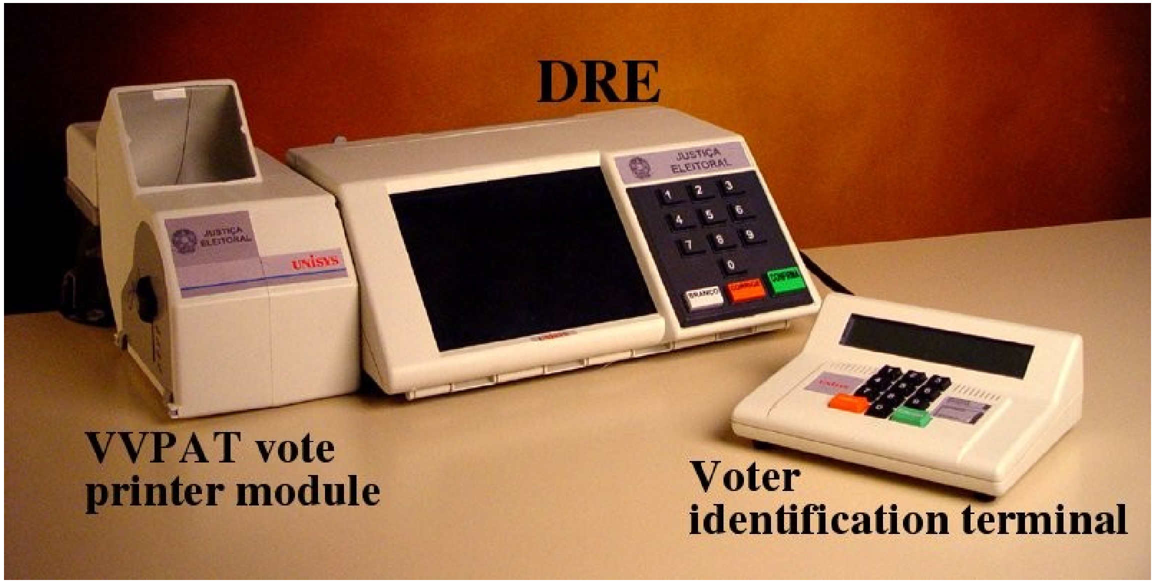
AUDIT
party sup.: sum(v.vt)= sum(p.vt)?

AUDIT
party sup.: sum(v.rp)= sum(p.rp)?

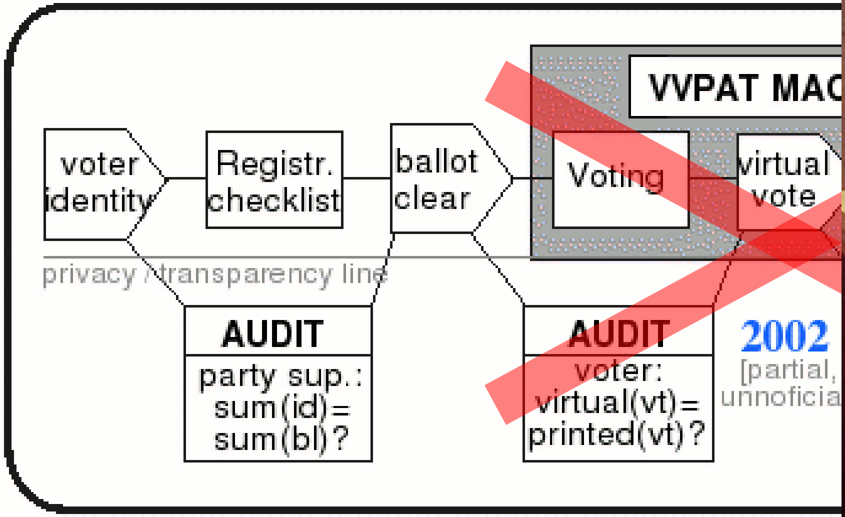
cast-as-intended

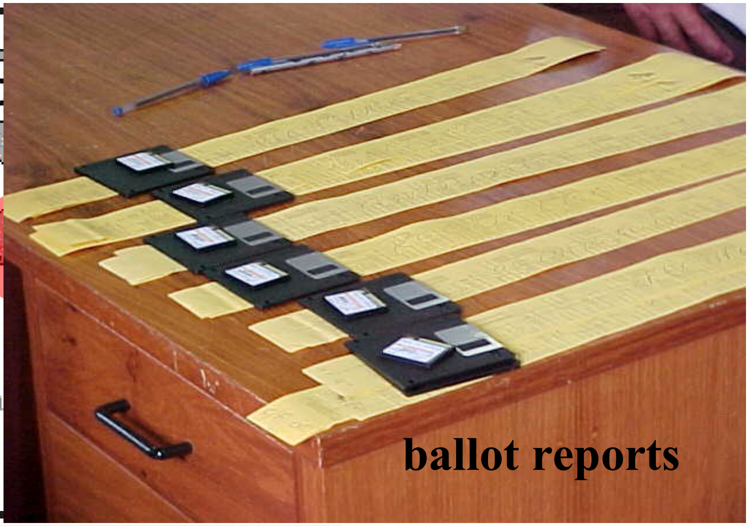
counted-as-cast

DRE adapted
to VVPAT
(Voter-Verifiable
Paper Audit Trail)

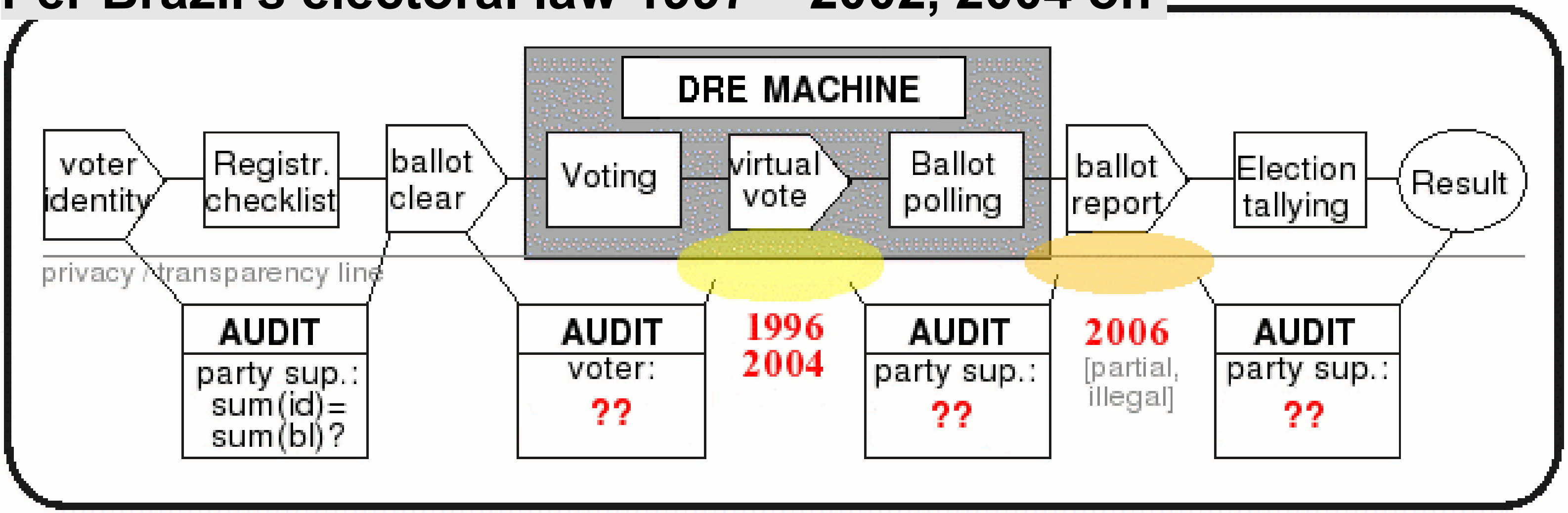


Evolution of a model





Per Brazil's electoral law 1997 – 2002, 2004 on



With DREs ...

An **Indetermination Principle – MIP** – apply

[similar to Gödel Incompleteness theorem in Logic,
Heisemberg's principle in Quantum Mechanics, etc.]

MIP: Vote secrecy and tallying integrity are mutually exclusive guarantees that a purely electronic voting system can offer.

Presented and defended by **Rebecca Mercury** in her
PhD thesis on Computer Science at U. of Pennsilvania, 2000
http://www.notablesoftware.com/Papers/thesdefabs.html

With DREs ...

MIP sets no hope for a system's

"*Thorough, verifiable chain of custody*"

"Thorough" in the sense of balancing risks for potentially conflicting interests involved: of at least two opposing candidacies, electoral officials, voters for clean elections.

Based on Level 4 assessment of ISO "Common Criteria" (ISO standard for security in information systems)

http://www.notablesoftware.com/checklists.html   http://csrc.nist.gov/cc

With DREs (corolary)...

MIP turn two conflicting senses of security

Inseparable and mutually cancelable:

First sense, that of voters (+ security experts on their behalf):
a) with rights to a secret ballot and to its correct tallying,
b) against manipulations of the electoral process,
c) by whoever in the electoral system,
d) which should be at least readily detectable by voter oversight;

Second sense, that of those in charge of the electoral process:
a) with rights to program or operate the electoral system,
b) against detection by voter oversight,
c) of whatever act, even if inept or in bad faith,
d) through which manipulations of the tallying is possible.

With DREs (corolary)...

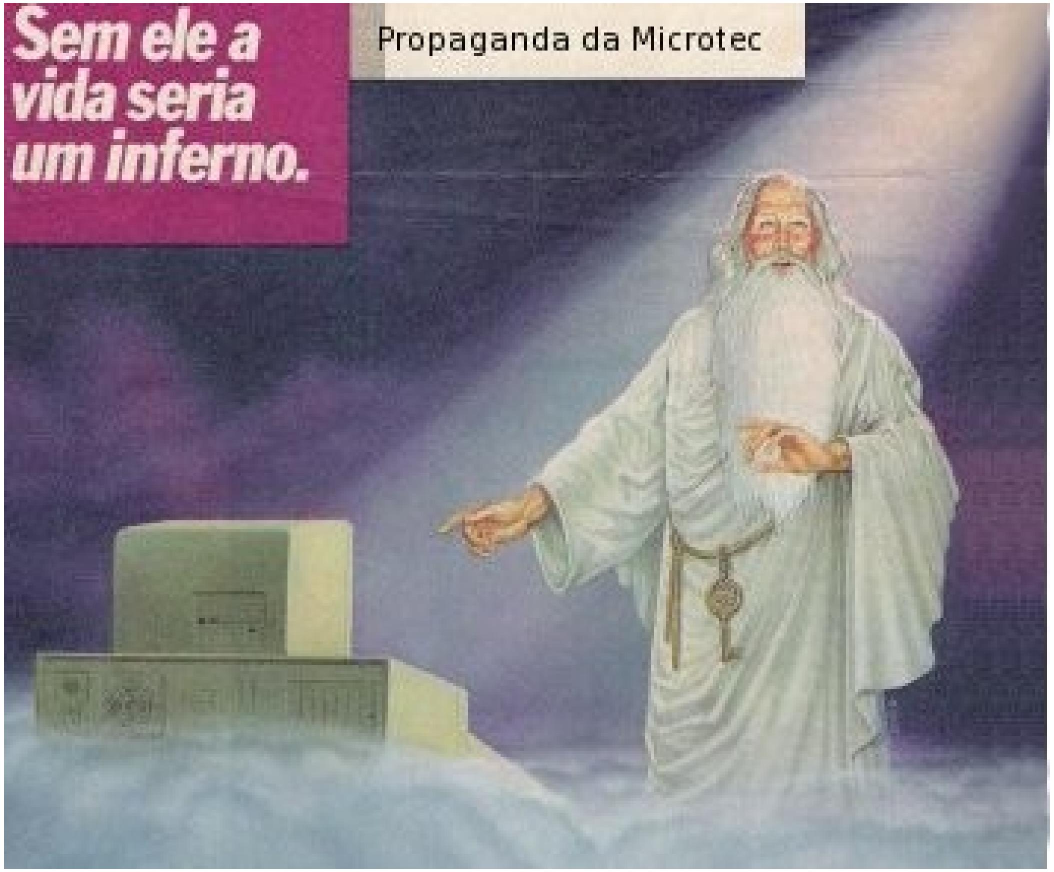
MIP vuelve dos sentidos conflitivos de seguridad

Inseparables y mutualmente cancelables:

Primer sentido, el de la seguridad de Electores:
a) con derecho a Voto y a la transparencia del pleito;
b) contra eventuales manipulaciones indebidas del proceso;
c) de cualquier origen o forma de alteración o abuso del sistema;
d) a través del cual estas puedan ser detectadas por estos.

Segundo sentido, el de la seguridad de ejecutores del proceso:
a) con derecho al acceso del sistema para programarlo, etc.;
b) contra eventuales detecciones por fiscalización/comprobación;
c) de cualquier desliz por incapacidad y/o mala intención;
d) a través de los cuales se pueda configurar un riesgo al pleito.

Saint Byte, circa 1987 (doctrine)



Propaganda da Microtec

Saint Byte today (doctrine)

Sem ele a vida seria um inferno.
Propaganda da Microtec

circa 2007: Turn the MIP into fable;

Turn “*Thorough, verifiable chain of custody*” into act of faith

Balanced VVPAT: (science)

End-to-end (**E2E**) cryptographic independent verification is a mechanism that can be built into elections to allow voters to take a piece of the ballot home with them as a receipt. This receipt **does not** allow voters to prove to others how they voted, but it **does** permit them to:

* Verify that they have properly indicated their votes to election officials (cast-as-intended).

* Verify with extremely high assurance that all votes were counted properly (counted-as-cast).

Examples: **Punchscan** (Chaum), **ThreeBallot** (Rivest)

References

Portal with articles by autor:

www.cic.unb.br/docentes/pedro/sd.php

Fórum do voto eletrônico:

www.votoseguro.org

E2E: punchscan.org

en.wikipedia.org/wiki/ThreeBallot

CIVILIS