Elections over Internet
Millions of flies can't be wrong

Lutz Donnerhacke

dig +dnssec naptr 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa

IKS

Election Requirements

Everyone can vote

Check the results

Hard to fake

Only one / region
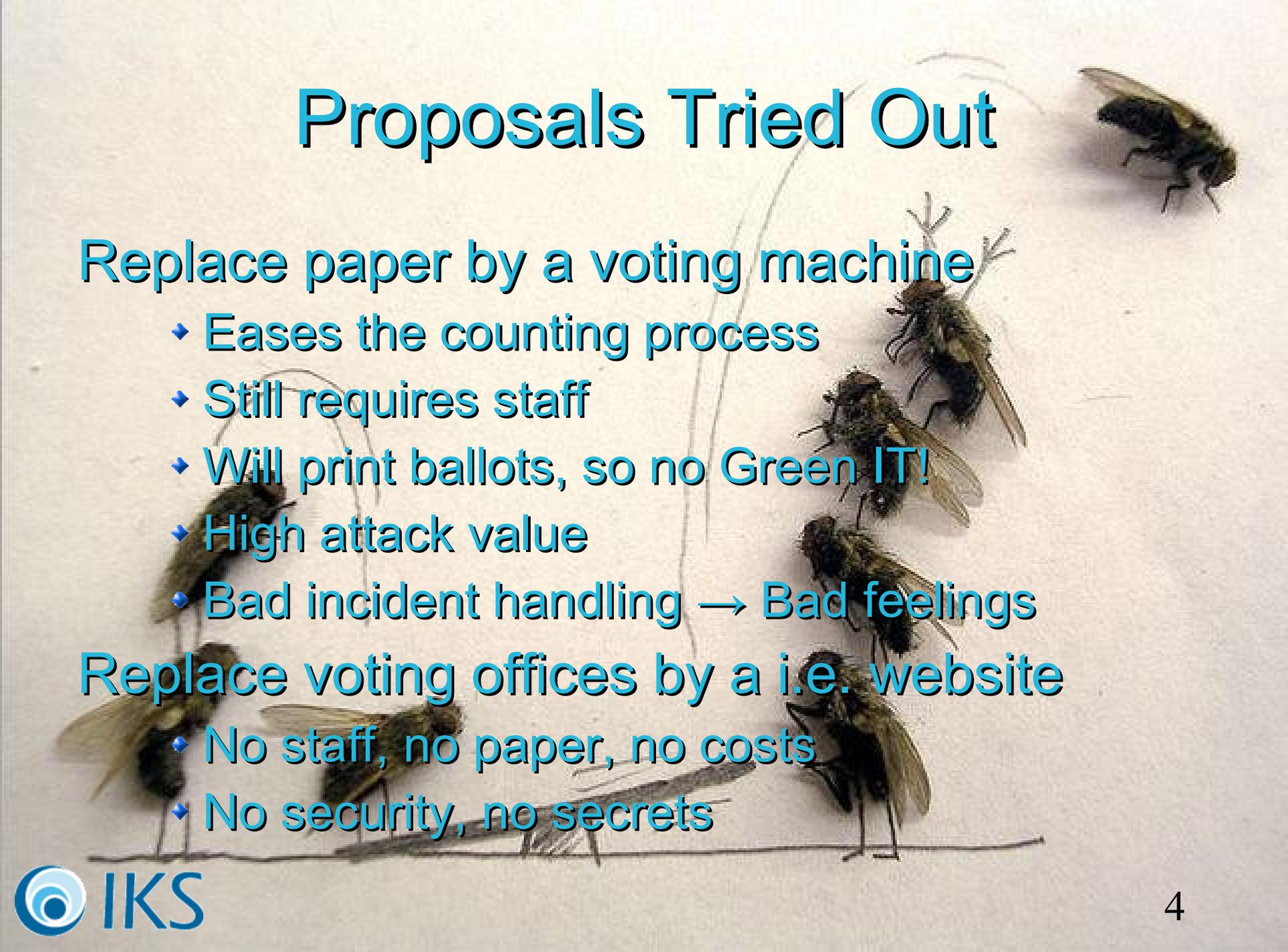
Untraceable votes

Easy to use

Traditional Approach

Paper based elections are hard
- To prepare (even fixing mistakes)
- To organise (needs trustworthy staff)
- To secure (more votes than voters, …)
- To verify (was *my* vote counted?)

But they are **The Symbol of Democracy**
- Easy to use every time and everywhere

IKS

3

Proposals Tried Out

Replace paper by a voting machine

- Eases the counting process
- Still requires staff
- Will print ballots, so no Green IT!
- High attack value
- Bad incident handling → Bad feelings

Replace voting offices by a i.e. website

- No staff, no paper, no costs
- No security, no secrets

IKS

4

Elections Broken Down

Hand out a localized voting permit
- Build a voter database
- Distribute *keys* (face2face, mail, or e-mail)

Hand out ballot papers
- Check against keys and voter database
- Hand out a *single* ballot to each voter

Collect votes and count them
- Supervise the voting and post processing

IKS

5

Switching To Internet

Keep the process: It's the nerve of voting

Use certificates instead of voter database
- Regional registration agent hierarchy

Use blind signatures instead of paper ballots
- Voter chooses an unique ID for the ballot
- Nobody else knows this ID

Use the signed ballot as key for voting
- Pseudonymous voting

Keep it trustworthy: Publish everything

IKS

6

Staff Requirements

System depend on official documents
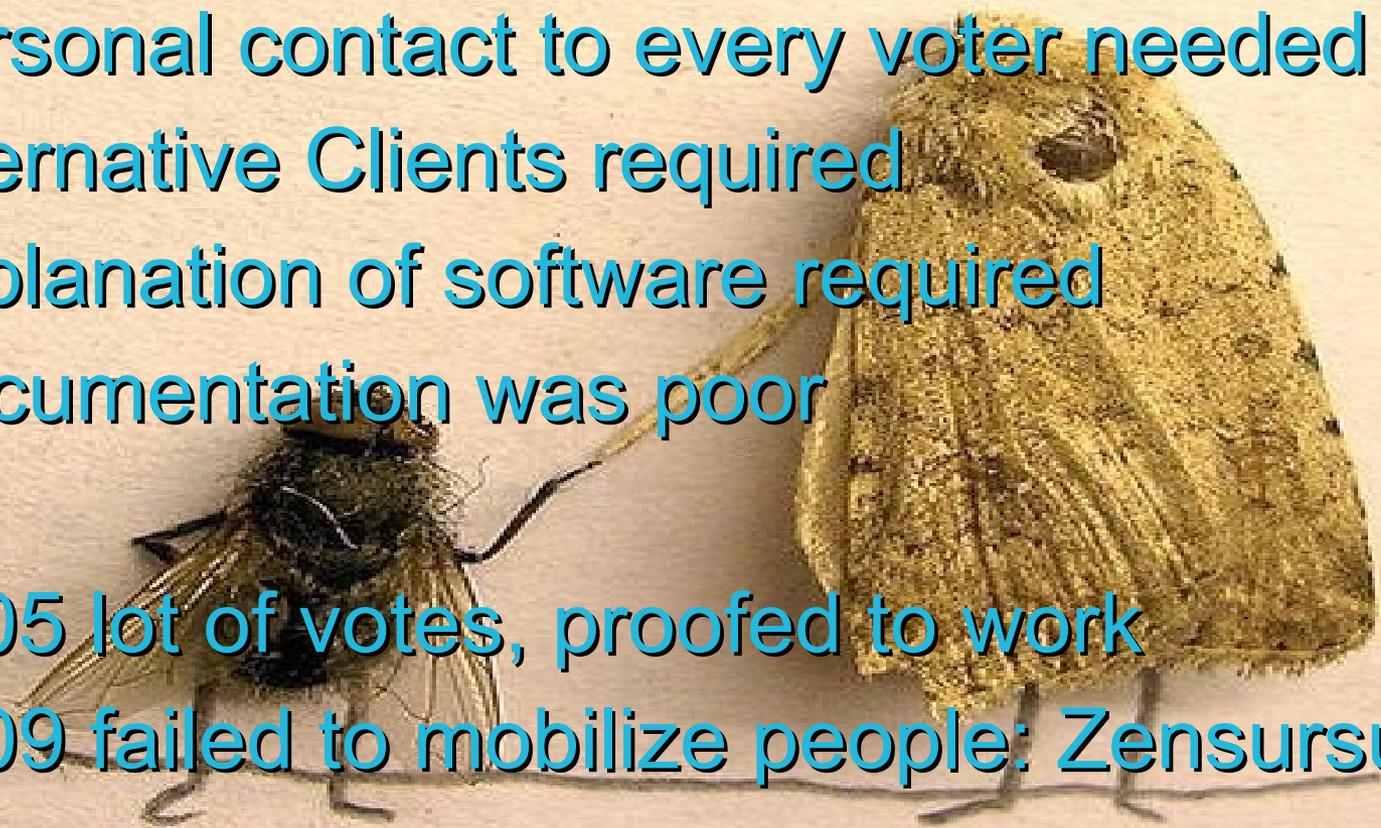
Personal contact to every voter needed

Alternative Clients required

Explanation of software required

Documentation was poor

2005 lot of votes, proofed to work

2009 failed to mobilize people: Zensursula

IKS

Media Coverage

Internet Election is a no-go in the press

German Angst dominates the discussion

Organized an election for children

- Huge work, classical paper ballots
- Strong cooperation with regional press
- Ask for help from all Bundestag members
- Coordinate rooms in plenty of towns
- Instruct helpful people what to do

Only to push the Internet election into press

IKS

Build On Basics

Demand from inter-organisation use cases

System is redesigned: Customizable

Free for ad hoc elections

Pay for personalized access with storage

Hope to see you soon …

IKS

Questions?

IKS