Internet Voting in Estonia

Tarvi Martens
Chairman

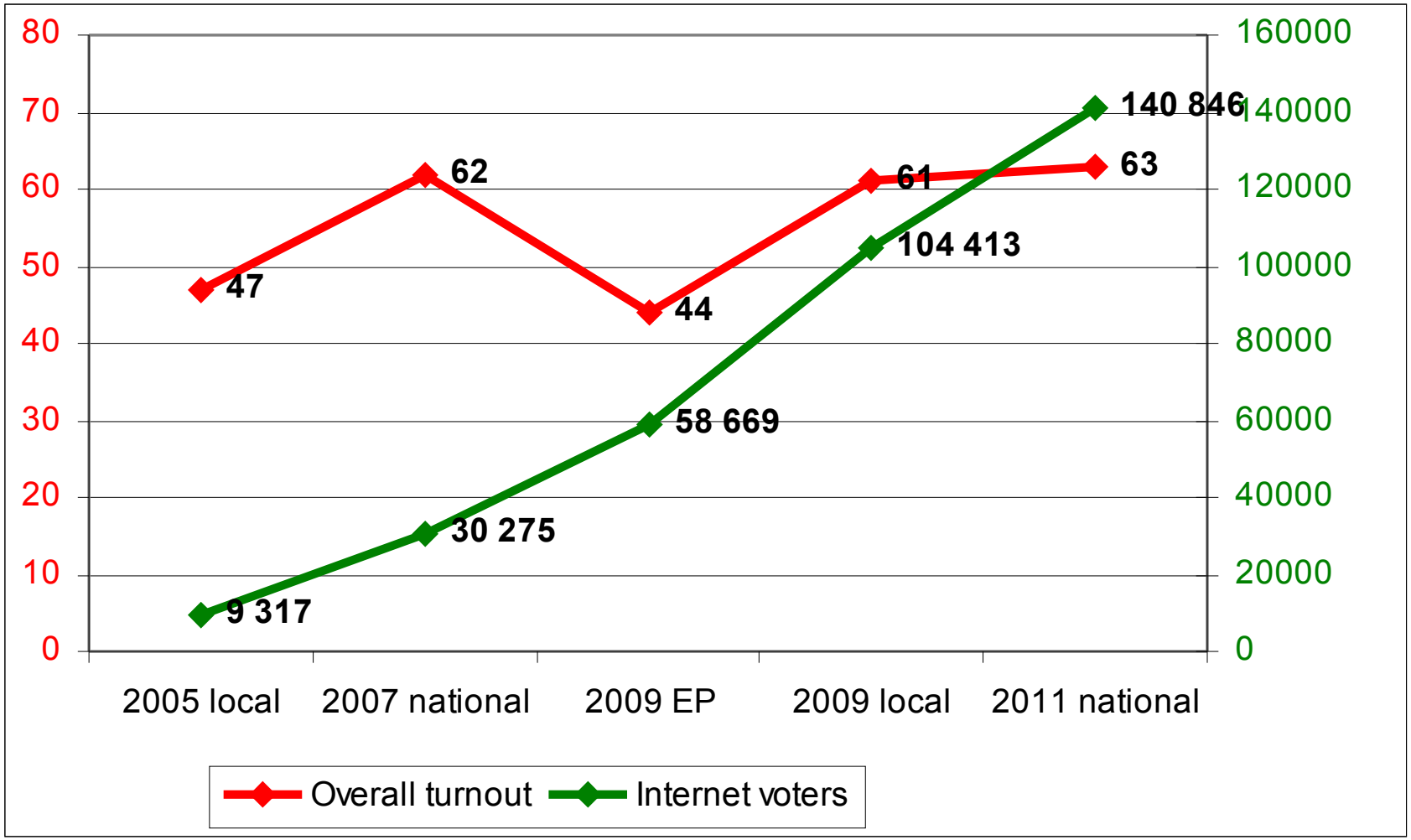
Electronic Voting Committee

Internet Voting?

- In October 2005 Estonia had first-ever pan-national Internet Voting **with binding results**

- Ever since, i-voting has been used in **five** elections in total

The spread of internet voting



ID-card Project

- Started in 1997
- First card issued: Jan 28, 2002
- October 2006: 1 000 000th ID-card was issued
  - “rollout completed”

The Card

- “Compulsory” for all residents

- Contains:
  - Personal data file
  - Certificate for authentication (along with e-mail address Forename.Surname@eesti.ee)
  - Certificate for digital signature

Usage of the ID-card

- Major ID-document
- Replacement of
  - (transportation) tickets
  - library cards
  - health insurance card
  - driver documents
  - etc...
- **Authentication token for all major e-services**
- **Digital signature tool**

Internet Voting ?

- Not a nuclear physics
- Just another application for ID-card

  ...with some special requirements & measures...

I-voting Main Principles

- All major principles of paper-voting are followed
- I-voting is allowed during 7-day (was: 3-day) period before Voting Day
- The user uses ID-card or Mobile-ID
  - System authenticates the user
  - Voter confirms his choice with digital signature
- Repeated e-voting is allowed
  - Only last e-ballot is counted
- Manual re-voting is allowed
  - If vote is casted in paper during pre-voting days, i-vote(s) will be revoked

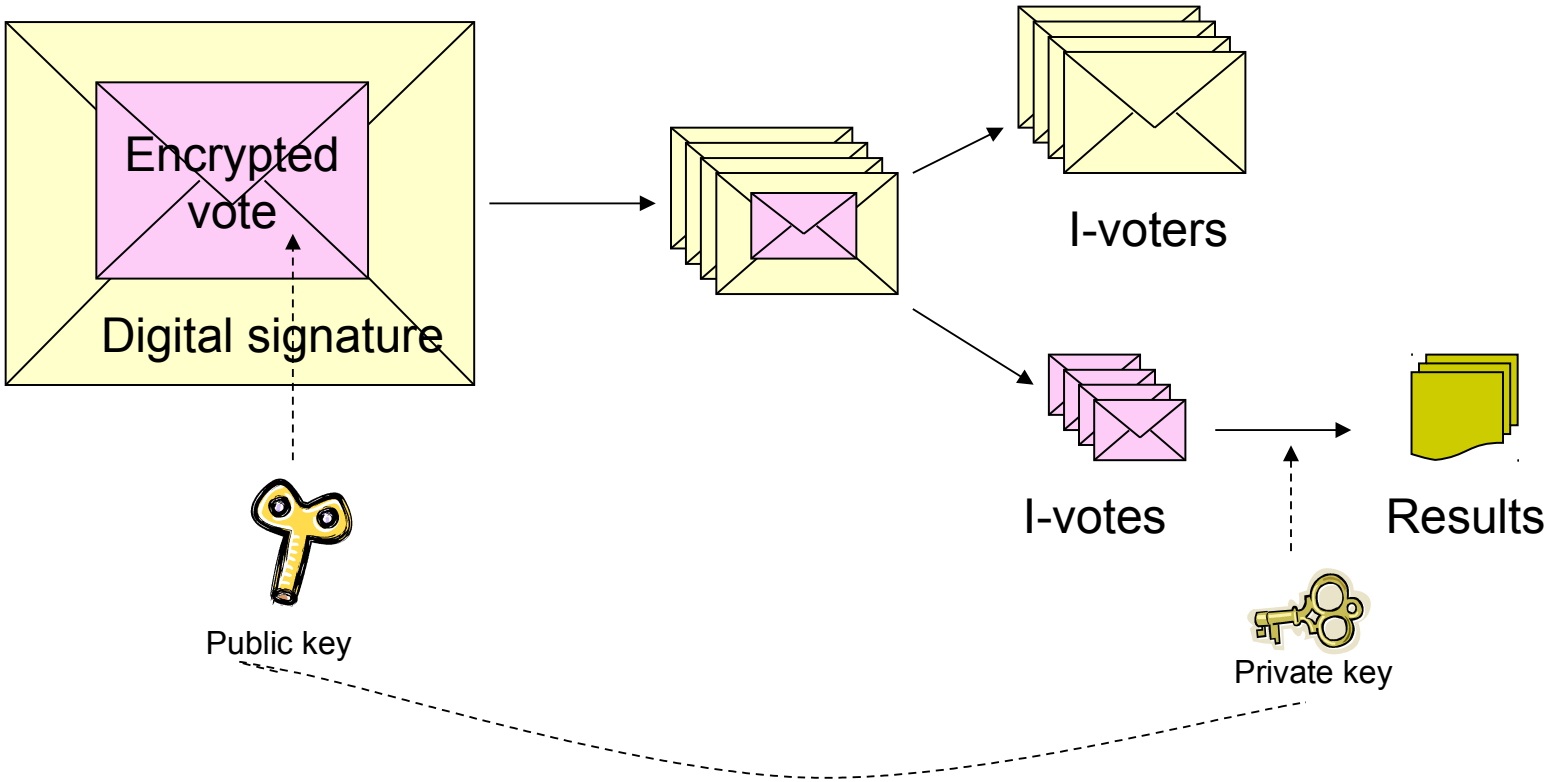
Voter registration

- Missing

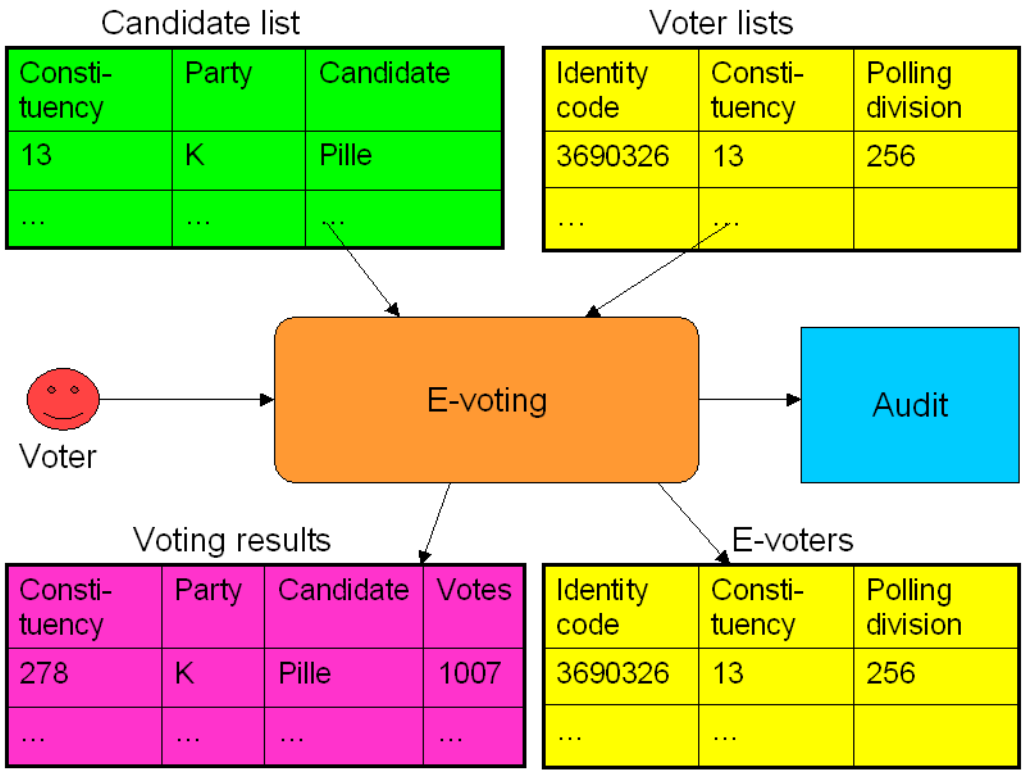
- All citizen (residents) should register their place of living in central population register
- Only voters with registered addresses are eligible

- Population register is used

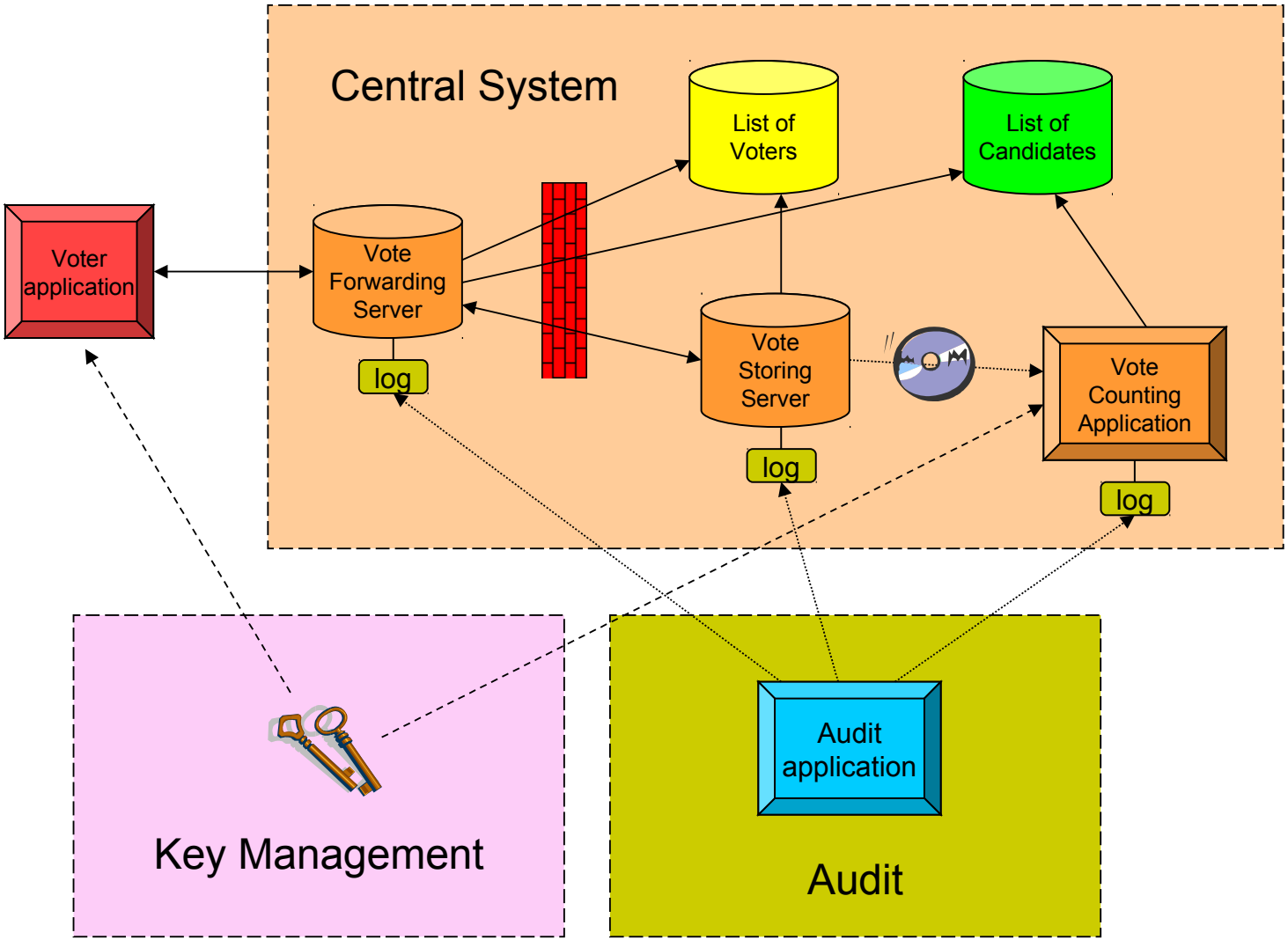
Envelope scheme



Scope of the I-voting system



Architecture



Cancellation of i-votes

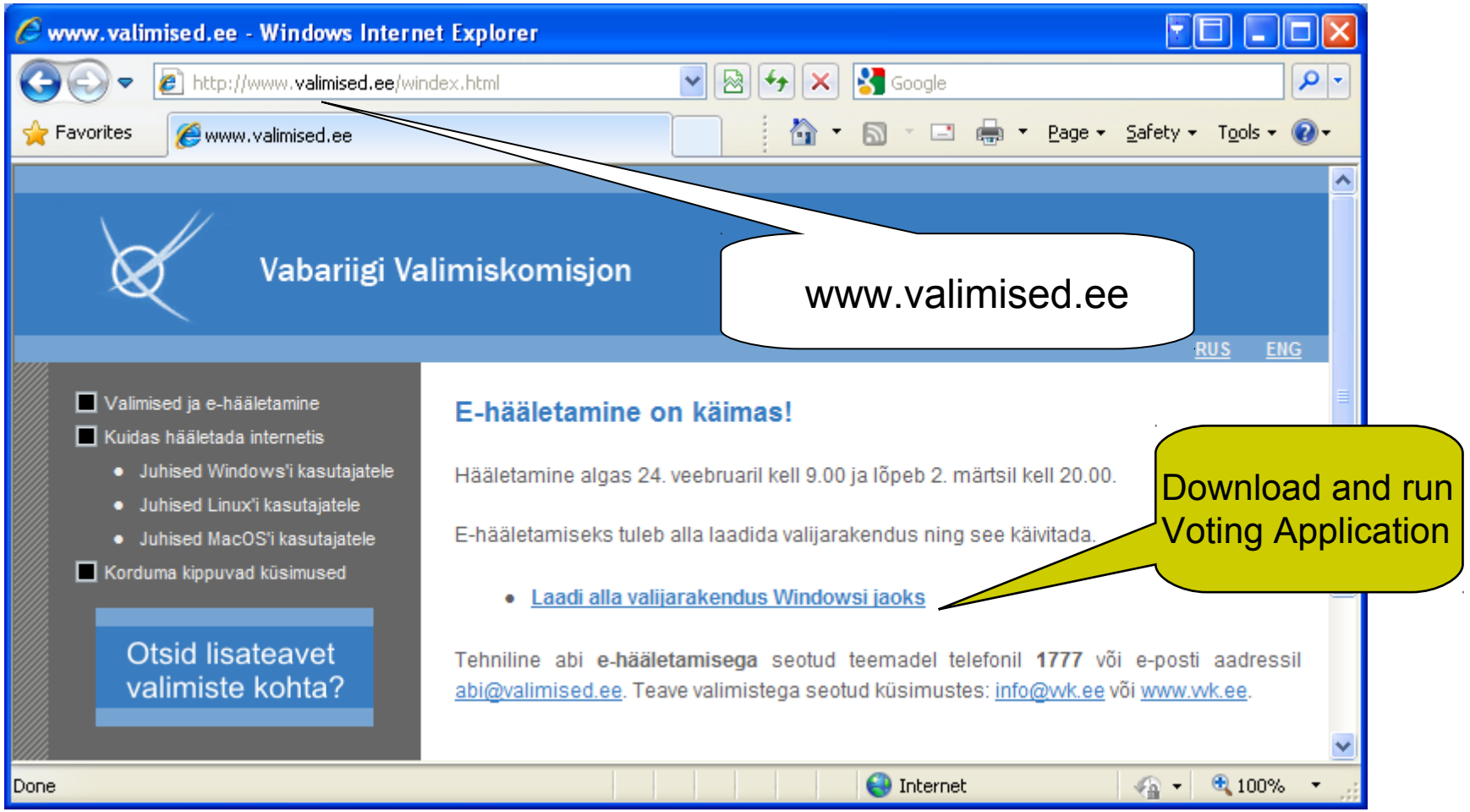
All Internet Voters' lists are printed and sent to polling stations two days before Election Day

Polling stations check the polling lists for possible Internet Voters who voted in the polling station on paper and mark all Internet Voters in the polling station list with "E"

If a double voter is found a note of cancellation is drafted in the Election Infosystem by the polling station and the I-vote is cancelled centrally

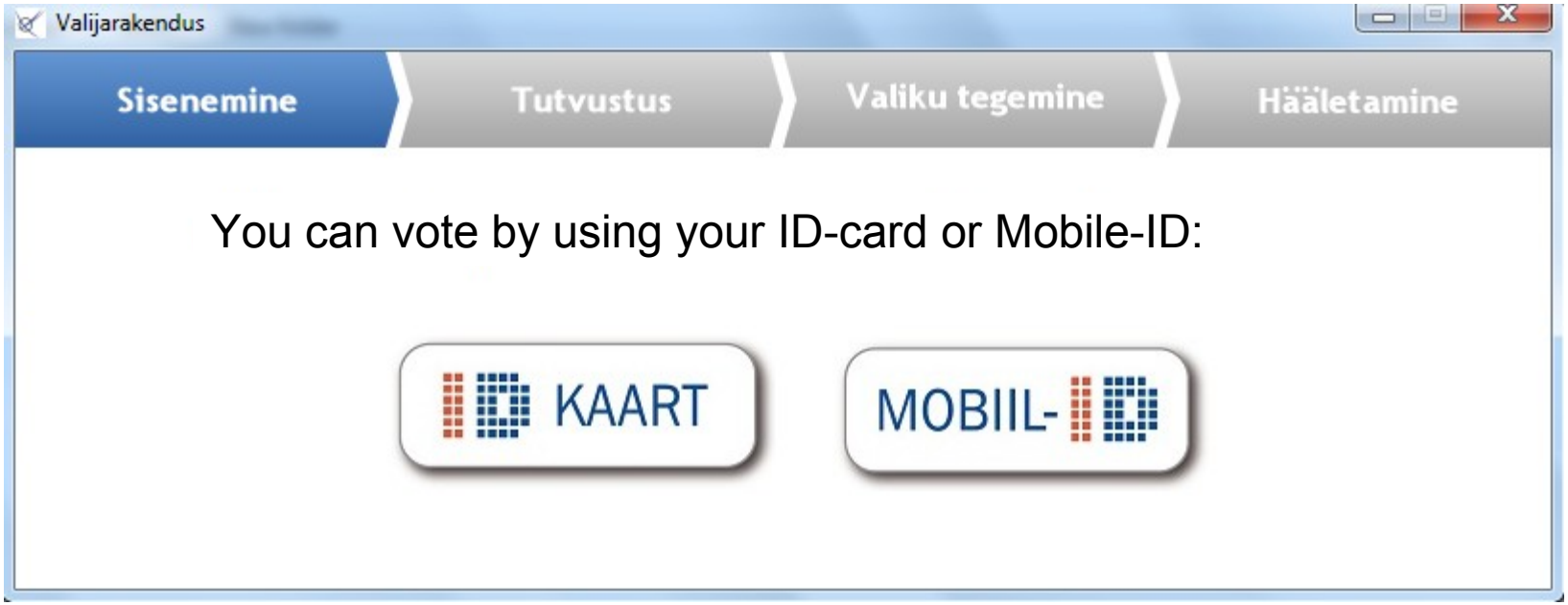
User view

Website for voting



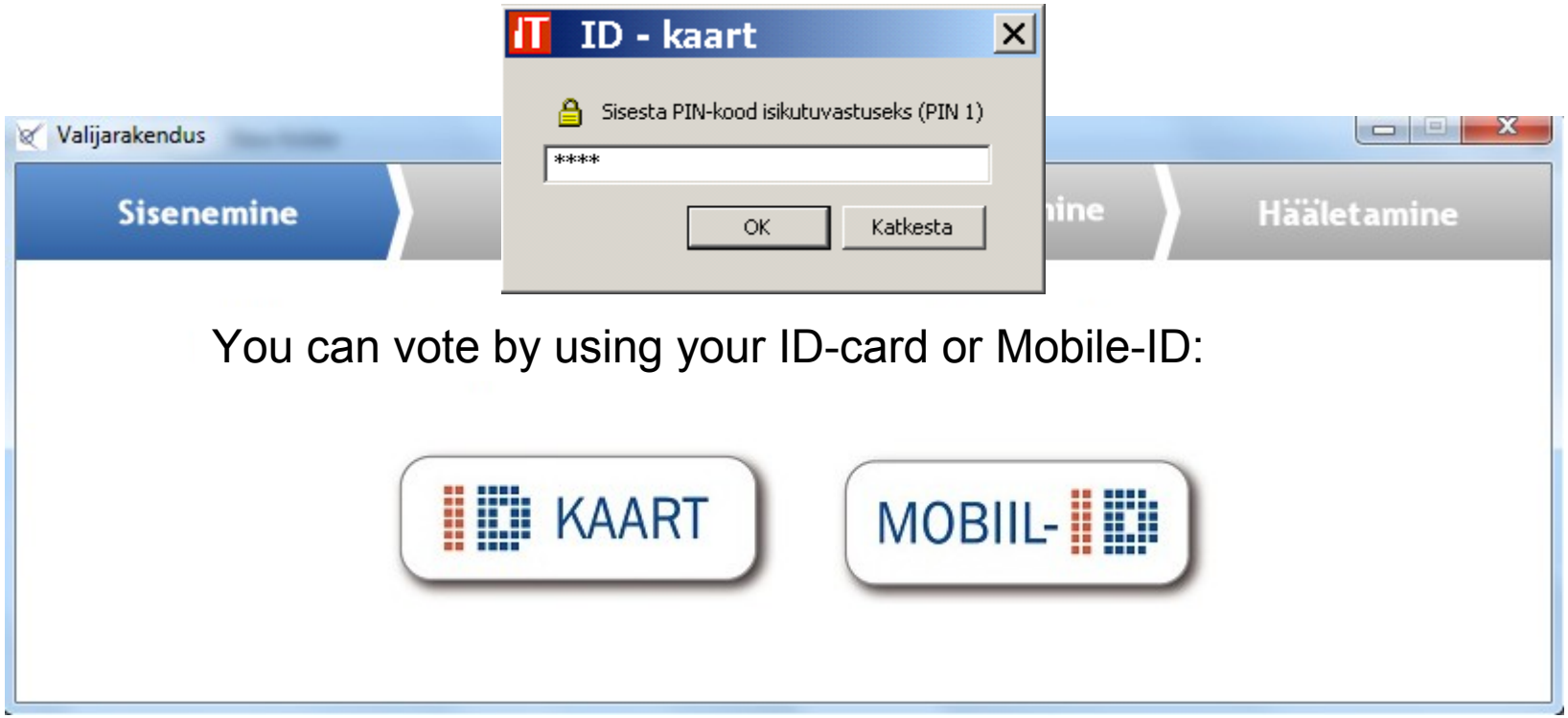
Run the Application

- Select your eID



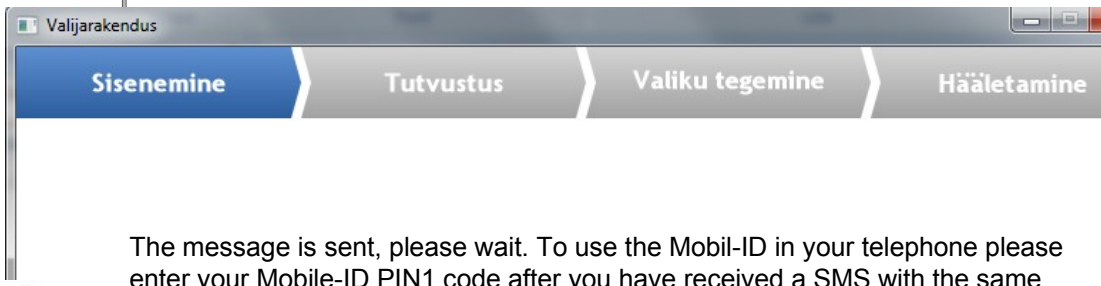
In case of ID-card... ****

- **Put your card into card reader**
- **Insert PIN 1**



In case of Mobile-ID...

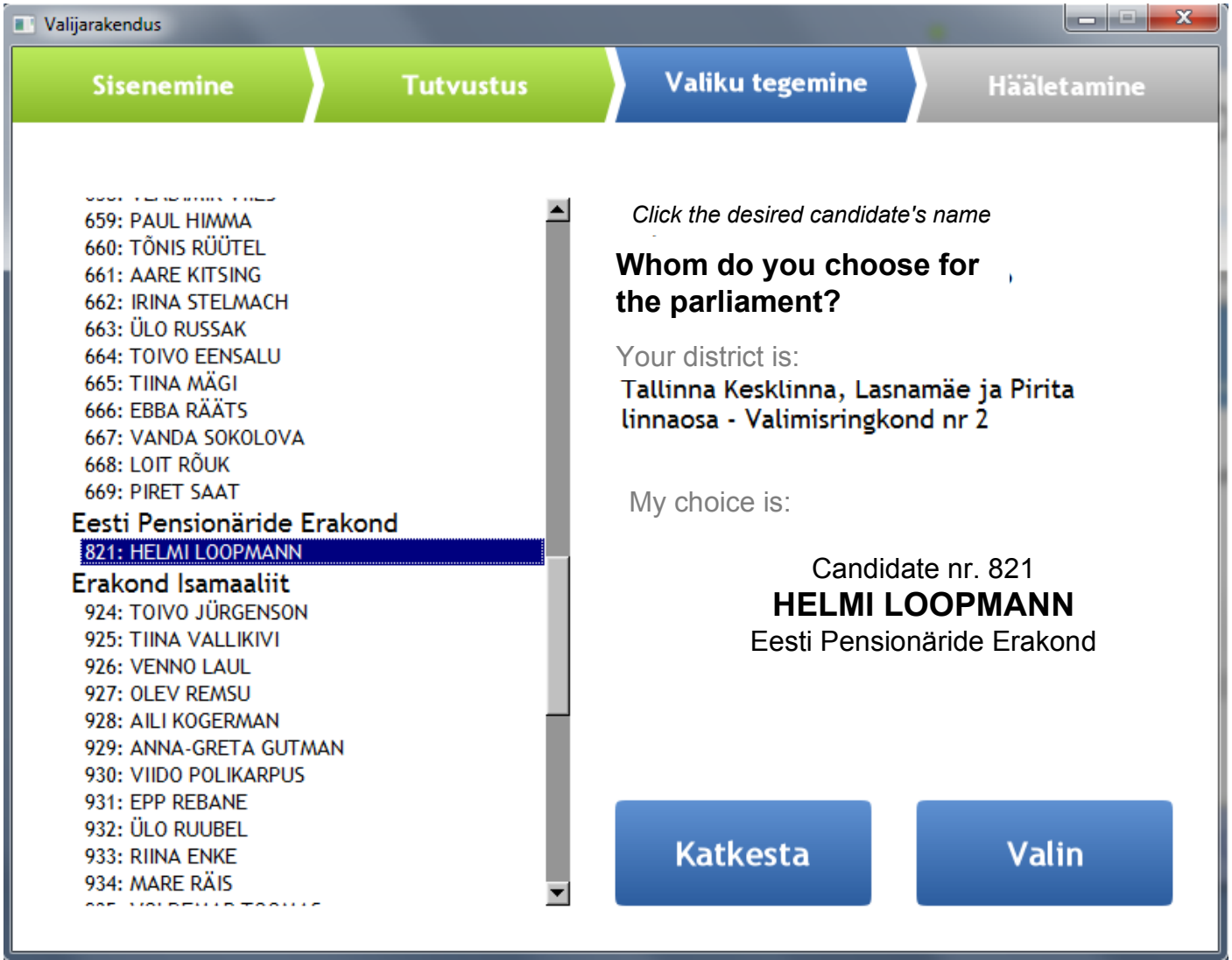
- Enter phone number
- Verify verification code
- Insert PIN 1



You are identified

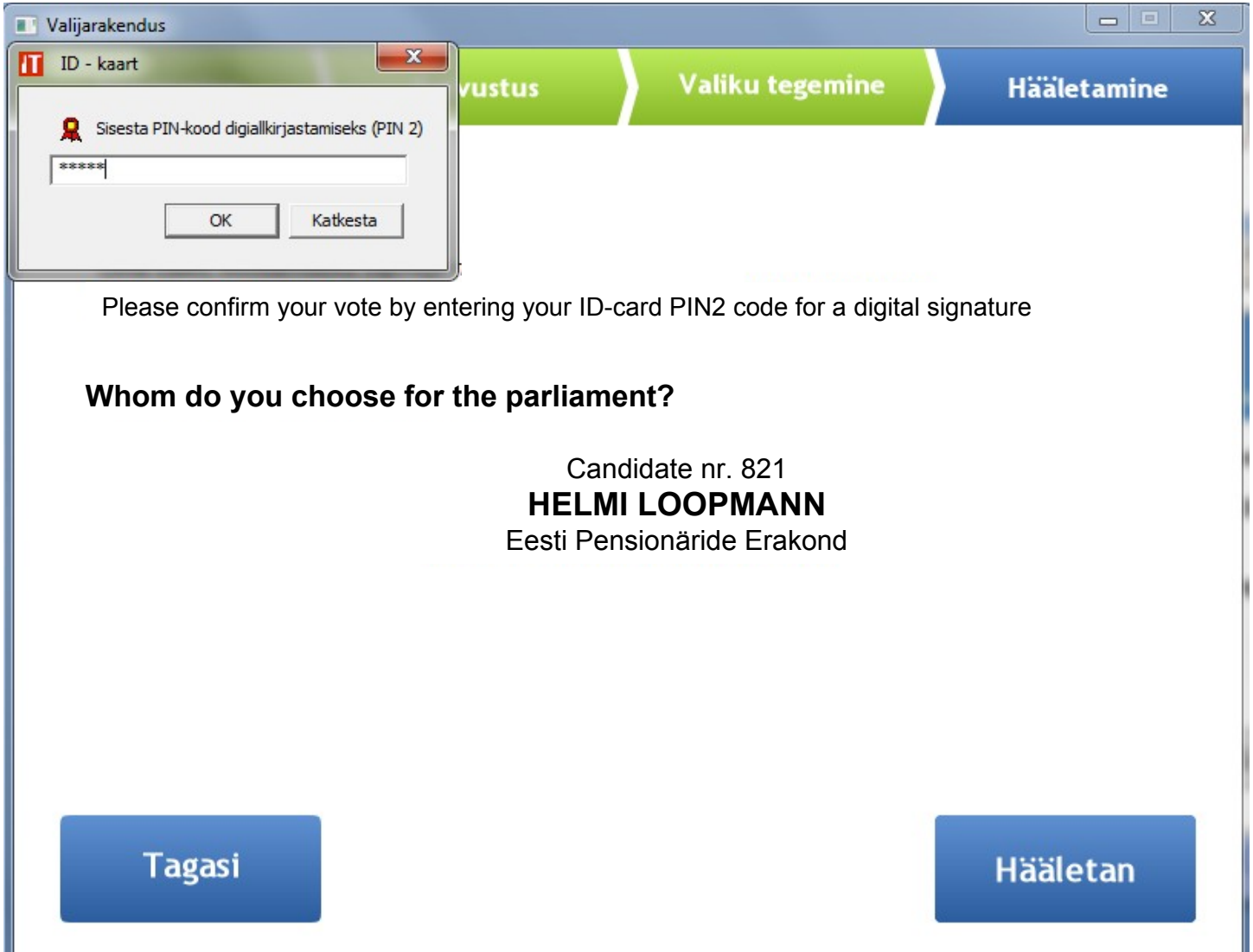
Ballot completion

- **Choose a candidate**



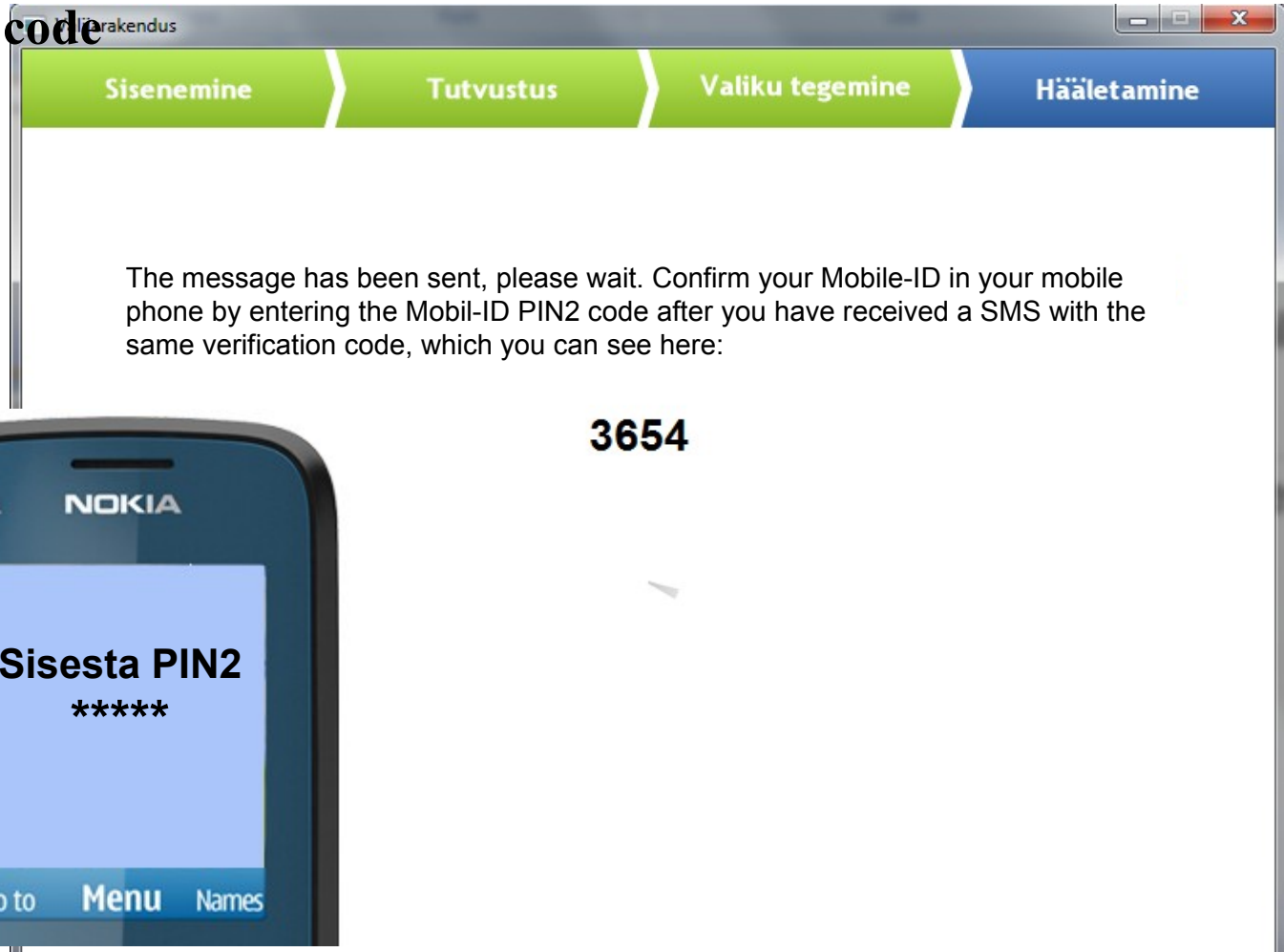
Confirmation (ID-card)

- **Confirm your choice with PIN2**

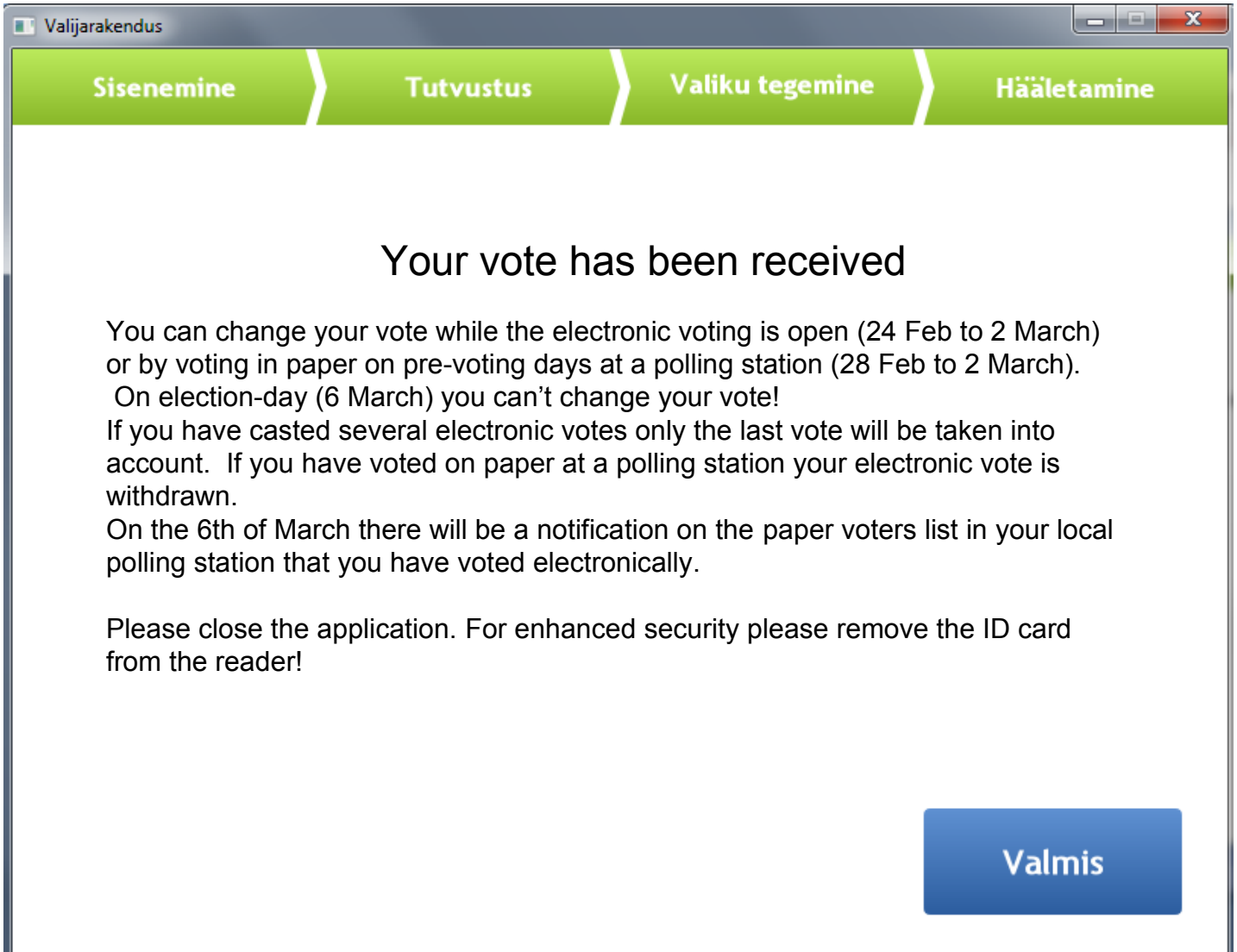


Confirmation (mobile-ID)

- Confirm your choice by signing digitally
- Verify verification code
- Insert PIN 2

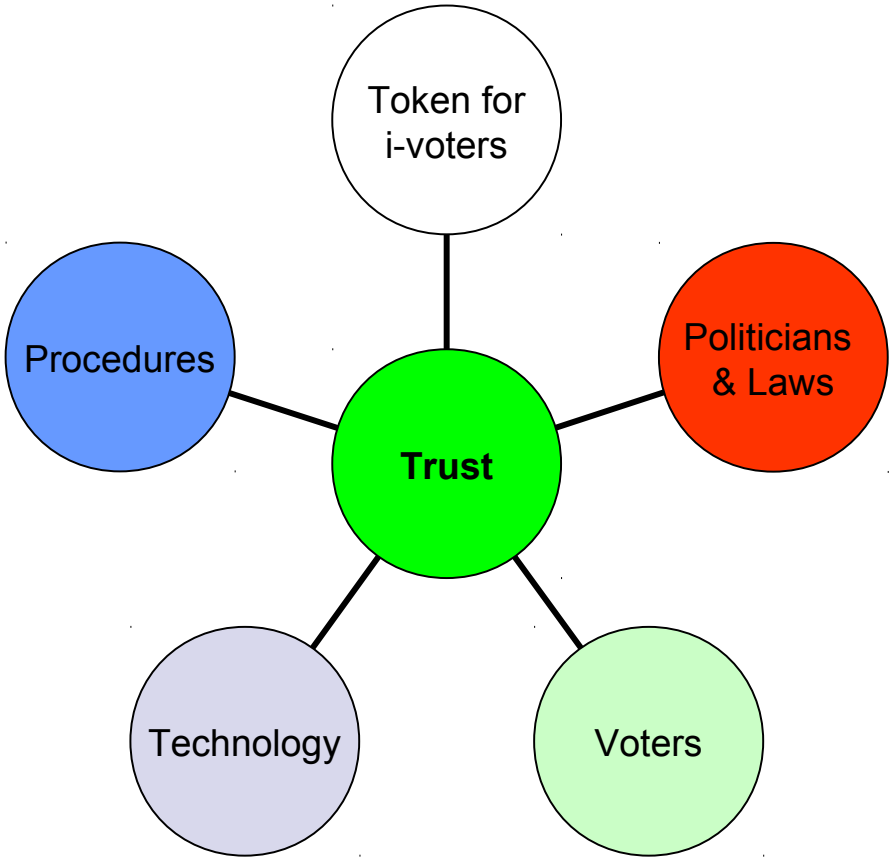


Vote received



On principles

What it takes ?



Principle of Transparency

- All system components shall be transparent for auditing purposes
- No “black boxes” are allowed
  - No use of 3rd party-controlled authentication mechanisms or services
  - No components without source code

Technology Selection

- Keep it as simple as possible
- Build it on secure & stable platforms (Debian)
- Use widely known programming languages
- No fancy user interfaces for server operations

Managing Procedures

- All fully documented
- Crash course for observers-politicians & auditors
- All security-critical procedures:
  - Logged
  - Audited & observed
  - Videotaped

Hosting and Monitoring

- Governmental security hosting
- Strict requirements for entering the server premises
  - Auditor(s), cam-man, operator(s), police officer
- Sealing of hardware and data carriers
- Large number of network security specialists involved in network-monitoring 24/7 for dDOS or trojans in voluntary basis

Voter verifiability

New kid in the block

ˇVoting

(1): ID-card authentication

(2): List of candidates

(3): $Sig_V(Enc_S(Rnd,Vote))$

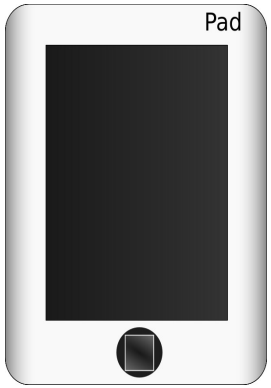
Voting with verification

(1): ID-card authentication

(2): List of candidates, OTP

(3): $Sig_V(Enc_S(Rnd,Vote))$

(4): Rnd, OTP



(5): OTP

(6): $Sig_S(Sig_V(Enc_S(Rnd,Vote)))$
List of candidates

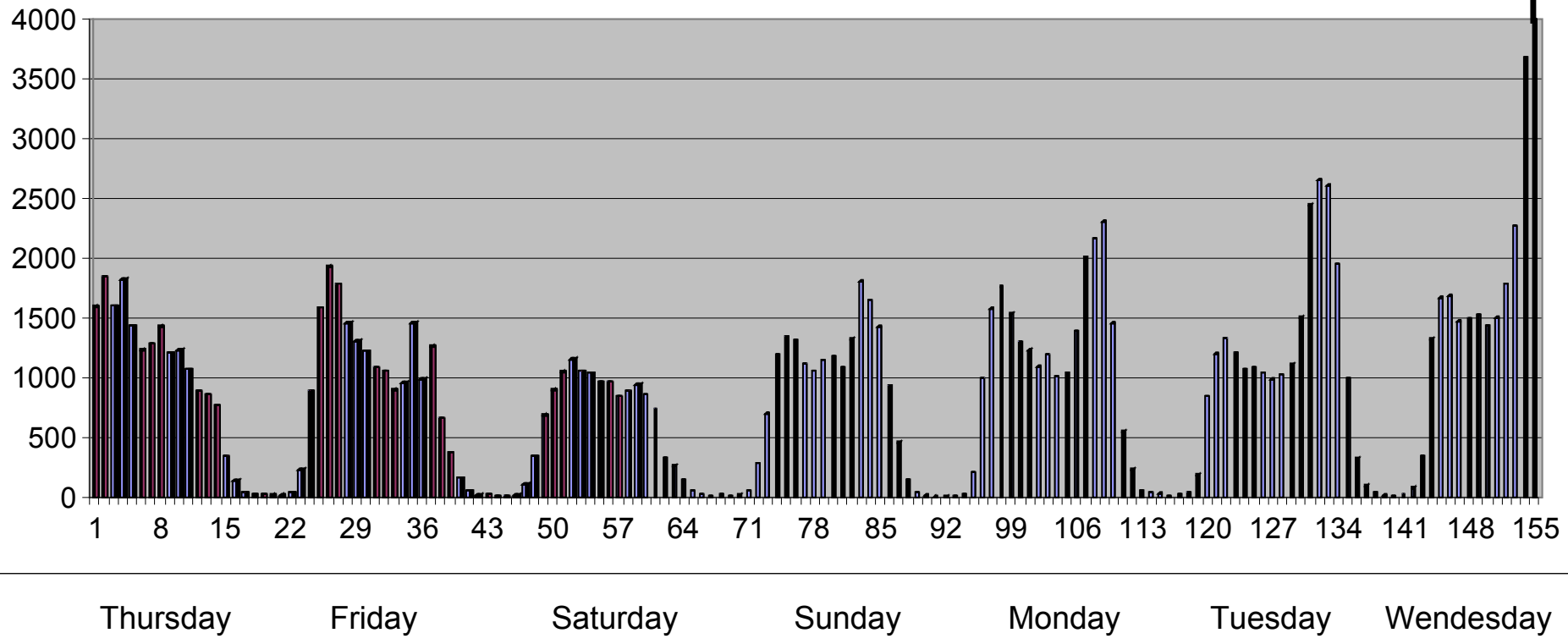
Verifiability

- The protocol is voter verifiable
- Voter has means to verify some of following properties about the ballot:
  - **Cast as intended**
  - **Accepted as cast**
  - Tallied as recorded
- Verifiability is needed to
  - discover real manipulation attacks
  - discourage potential real attackers

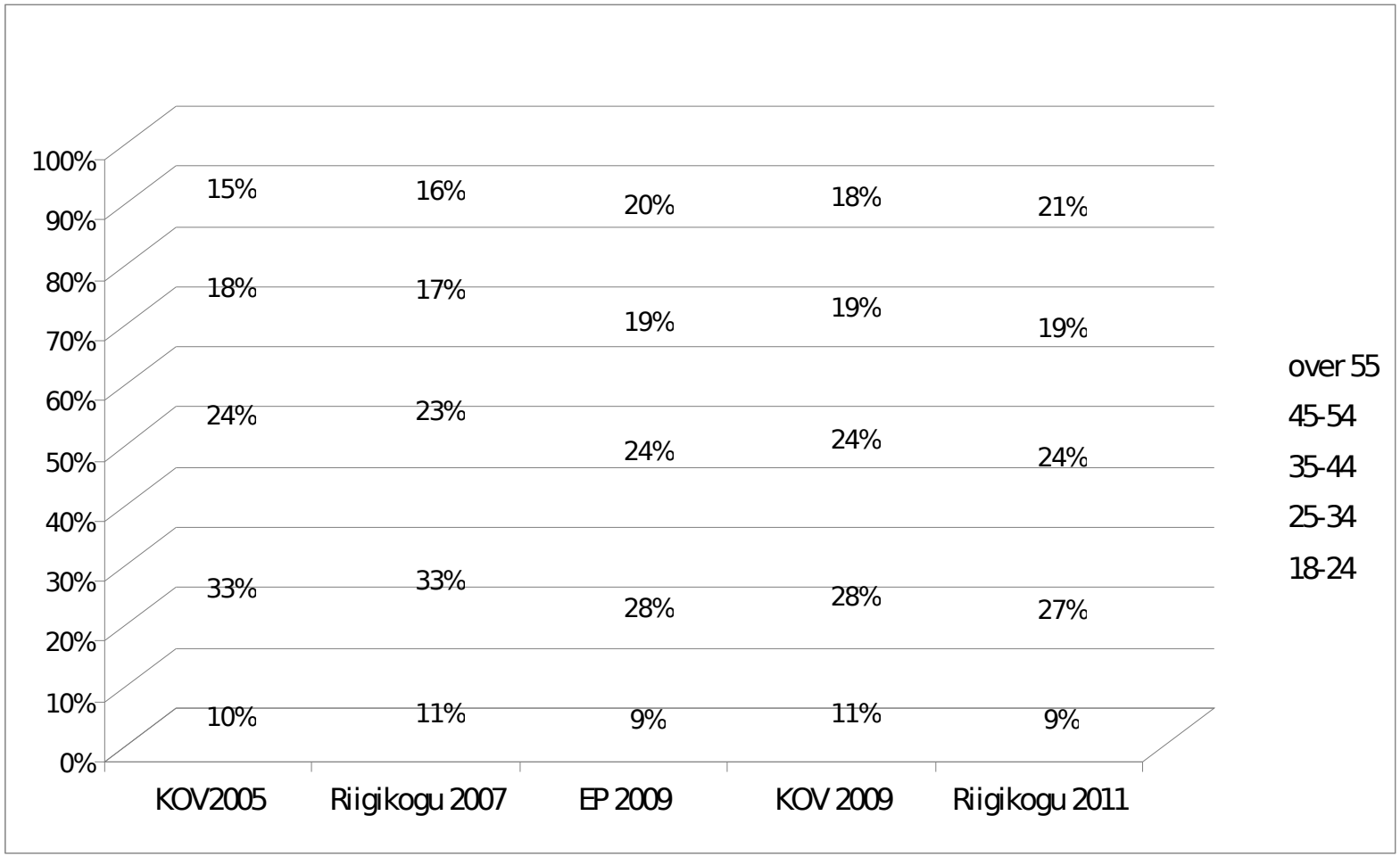
Statistics 2005..2011

Votes per hour, 2011

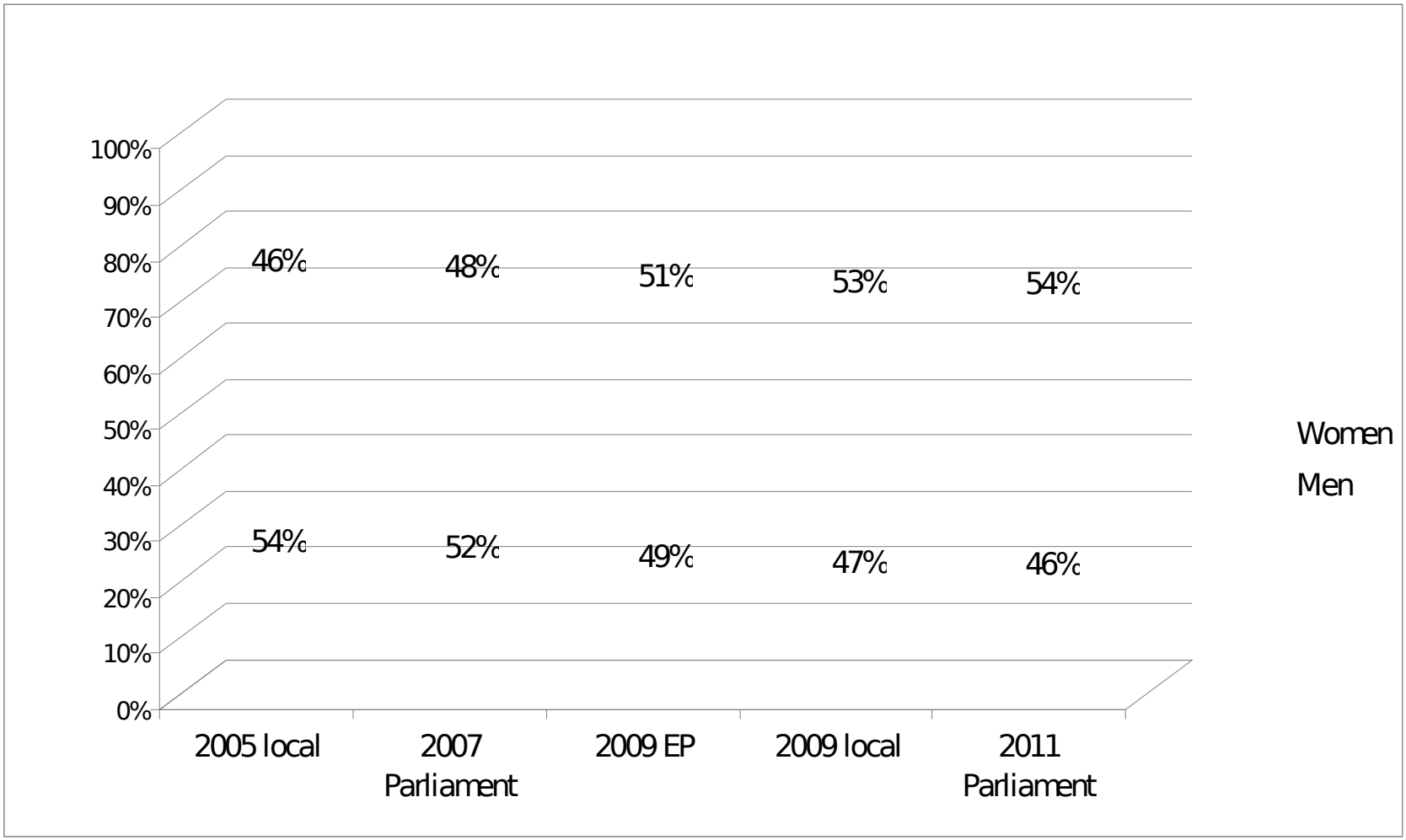
7081+98



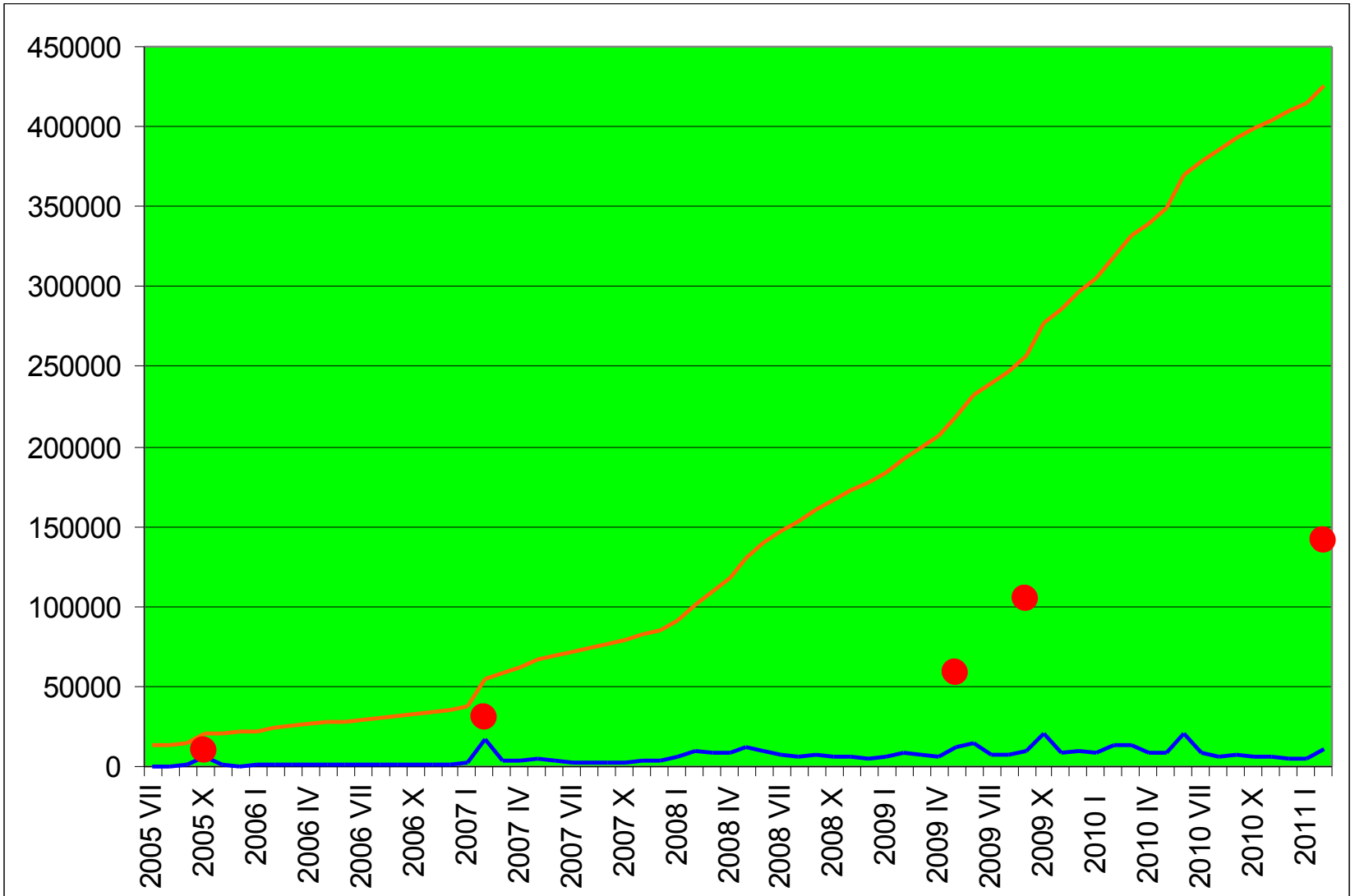
How old is the I-voter?



Sexual equality?



ID-card usage vs. I-voting



Lessons learned

- I-voting is not a killer-application.
  It is just another way for people to vote
- People's attitude and behavior change in decades and generations, not in seconds
- I-voting is as natural as Internet-banking but even more secure

- Internet voting is here to stay

More information

www.valimised.ee
www.vvk.ee

tarvi@sk.ee