

Internet Voting in Estonia



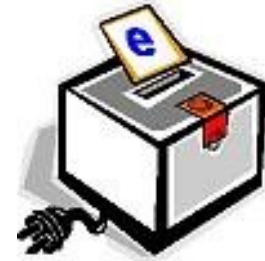
Tarvi Martens
Chairman

Electronic Voting Committee

Internet Voting?

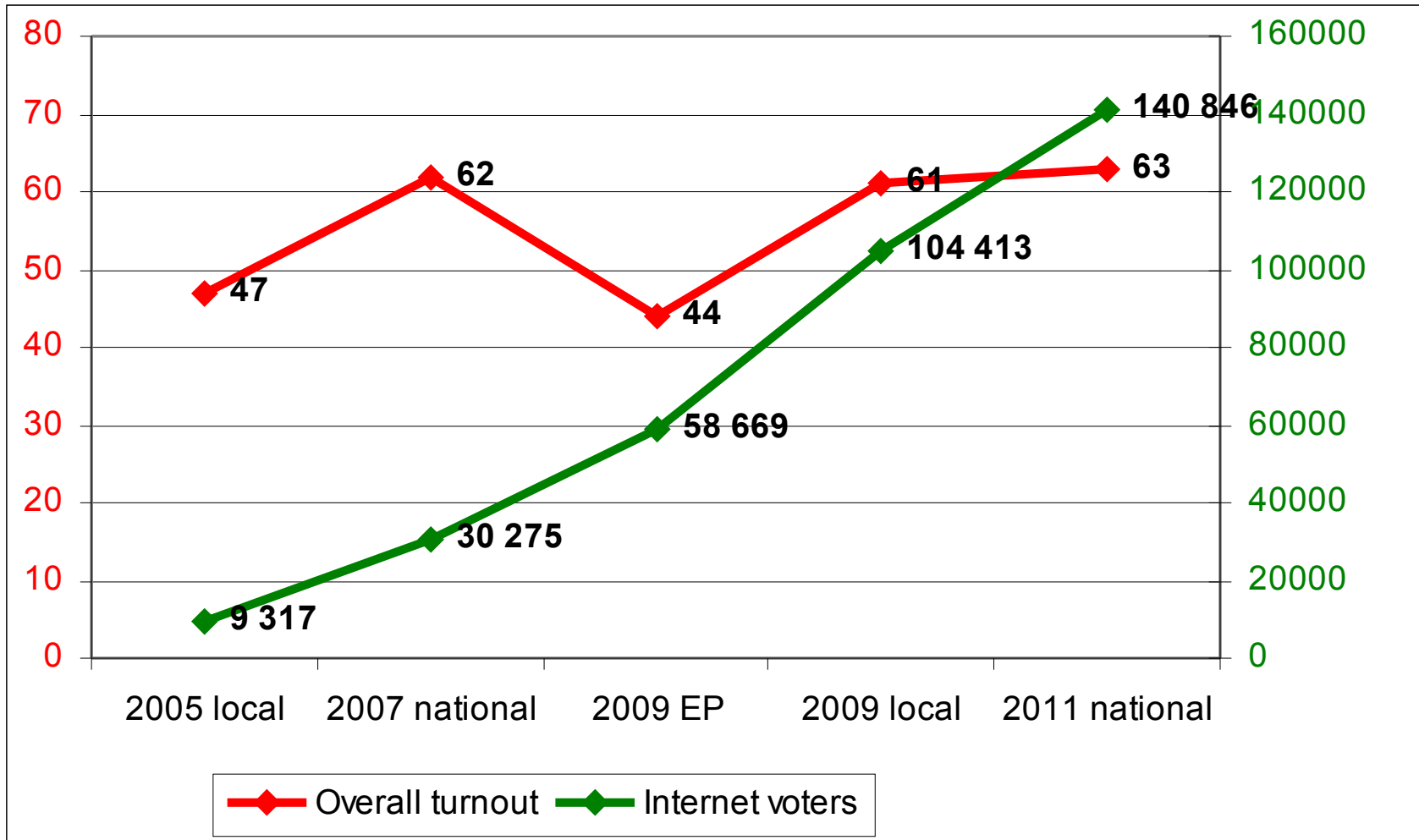


- In October 2005 Estonia had first-ever pan-national Internet Voting **with binding results**



- 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

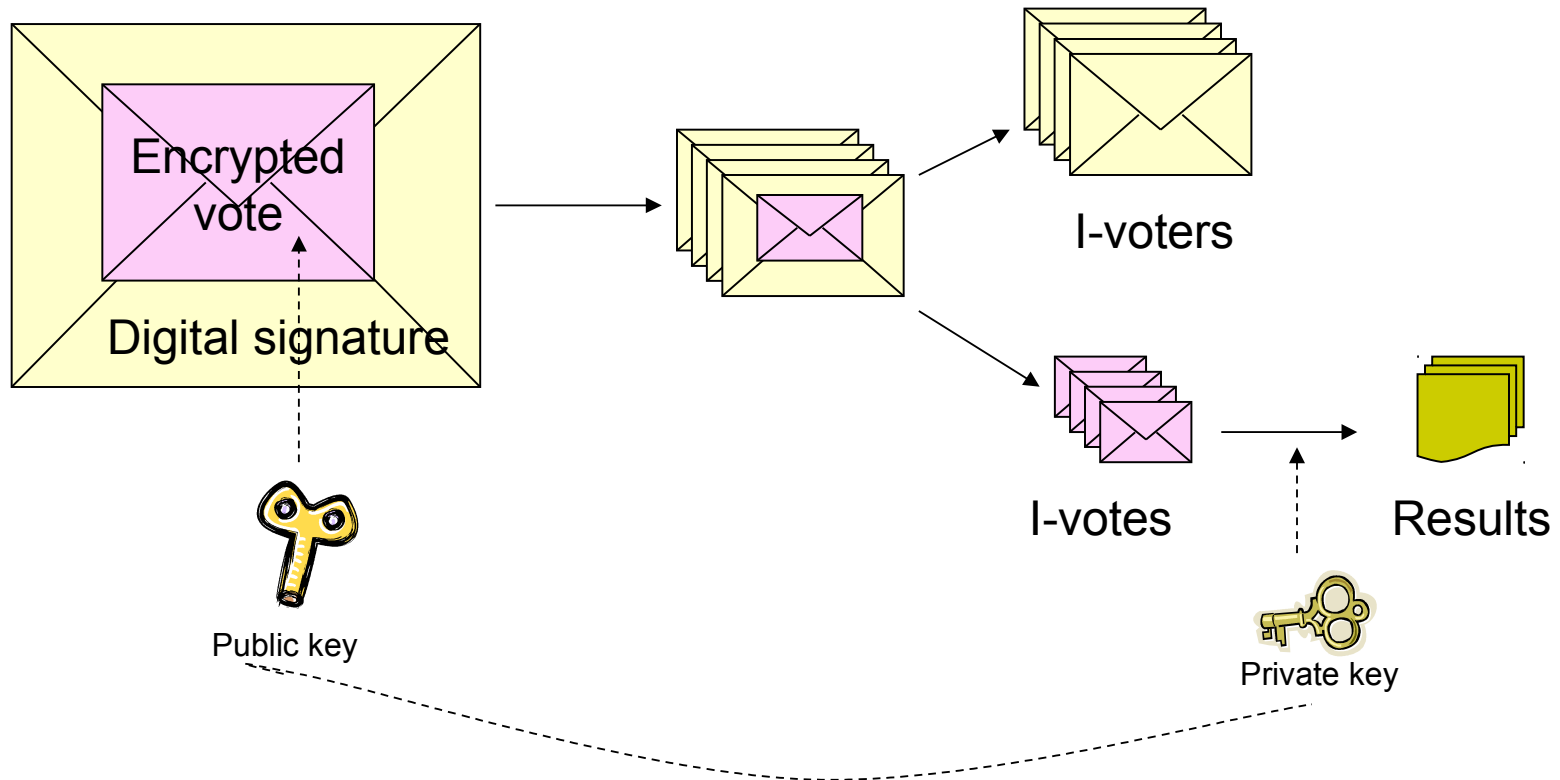
- All major principles of paper-voting are followed
- I-voting is allowed during 7-day (was: 3-day) period before Voting Day
- The user uses ID-card or Mobile-ID
 - System authenticates the user
 - Voter confirms his choice with digital signature
- Repeated e-voting is allowed
 - Only last e-ballot is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



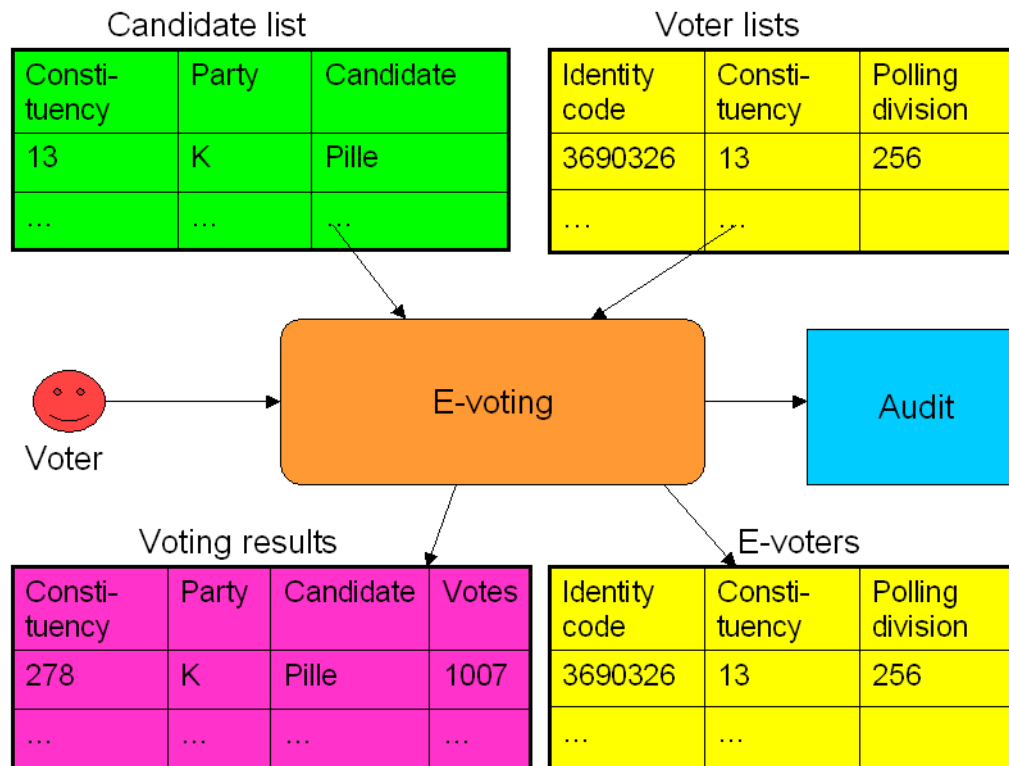
Voter registration

- 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

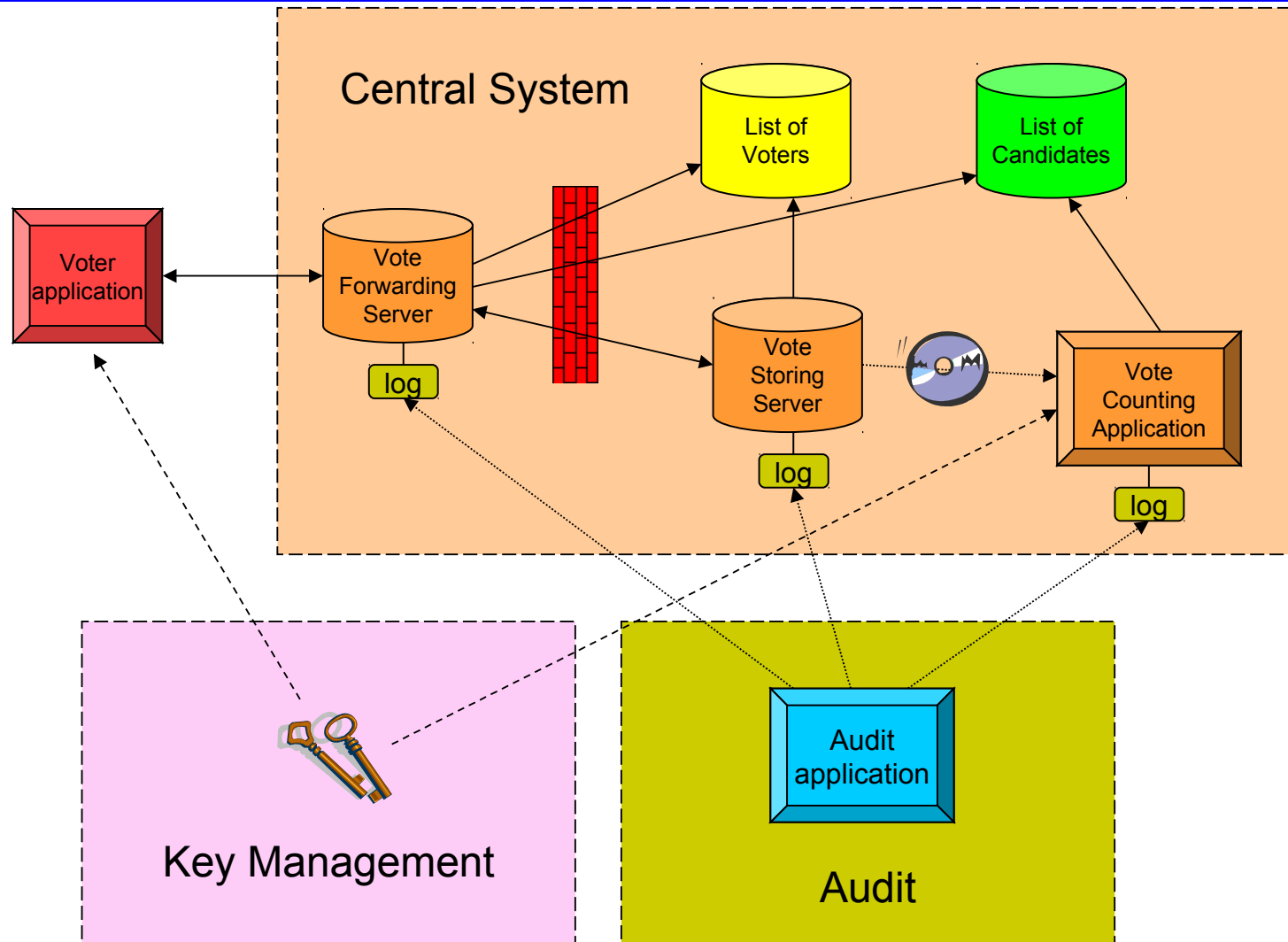
Envelope scheme



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



www.valimised.ee

E-hääletamine on käimas!

Hääletamine algas 24. veebruaril kell 9.00 ja lõpeb 2. märtsil kell 20.00.

E-hääletamiseks tuleb alla laadida valijarakendus ning see käivitada.

- [Laadi alla valijarakendus Windowsi jaoks](#)

Tehniline abi **e-hääletamisega** seotud teemadel telefonil **1777** või e-posti aadressil abi@valimised.ee. Teave valimistega seotud küsimustes: info@wk.ee või www.wk.ee.

Otsid lisateavet valimiste kohta?



Run the Application

- Select your eID



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



- Put your card into card reader
- Insert PIN 1



Valijarakendus

Sisenemine

Hääletamine

ID - kaart

Sisesta PIN-kood isikutuvastuseks (PIN 1)

OK Katkesta

You can vote by using your ID-card or Mobile-ID:

KAART MOBIIL-ID

In case of Mobile-ID...



arakendus

Sisenemine Tutvustus Valiku tegemine Hääletamine

Enter your telephone number

Telefoninumber

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

Valijarakendus

Sisenemine Tutvustus Valiku tegemine Hääletamine

The message is sent, please wait. To use the Mobil-ID in your telephone please enter your Mobile-ID PIN1 code after you have received a SMS with the same verification code, which you can see here:

7030



You are identified



Valijarakendus

Sisenemine Tutvustus Valiku tegemine Hääletamine

Welcome

Nimi: **PEETER HÄÄLETAJA**
Isikukood: **37012021234**

You are voting in the 2011 parliamentary elections. This is the official elections, where the electronic votes are equal to votes on paper. Following are the choices for candidates in your residence electoral district.

Katkesta Otsustama

Ballot completion



- Choose a candidate

Valijarakendus

Sisenemine

Tutvustus

Valiku tegemine

Hääletamine

659: PAUL HIMMA
660: TÕNIS RÜÜTEL
661: AARE KITSING
662: IRINA STELMACH
663: ÜLO RUSSAK
664: TOIVO EENSALU
665: TIINA MÄGI
666: EBBA RÄÄTS
667: VANDA SOKOLOVA
668: LOIT RÕUK
669: PIRET SAAT
Eesti Pensionäride Erakond
821: HELMI LOOPMANN
Erakond Isamaaliit
924: TOIVO JÜRGENSON
925: TIINA VALLIKIVI
926: VENNO LAUL
927: OLEV REMSU
928: AILI KOGERMAN
929: ANNA-GRETA GUTMAN
930: VIIDO POLIKARPUS
931: EPP REBANE
932: ÜLO RUUBEL
933: RIINA ENKE
934: MARE RÄIS

Click the desired candidate's name

Whom do you choose for the parliament?

Your district is:
Tallinna Kesklinna, Lasnamäe ja Pirita linnaosa - Valimisringkond nr 2

My choice is:

Candidate nr. 821
HELMİ LOOPMANN
Eesti Pensionäride Erakond

Katkesta

Valin

Confirmation (ID-card)

- Confirm your choice with PIN2



Valijarakendus

ID - kaart

Sisesta PIN-kood digiallkirjastamiseks (PIN 2)

OK Katkesta

Valikute loetelu

Valikute tegemine

Hääletamine

Please confirm your vote by entering your ID-card PIN2 code for a digital signature

Whom do you choose for the parliament?

Candidate nr. 821
HELMİ LOOPMANN
Eesti Pensionäride Erakond

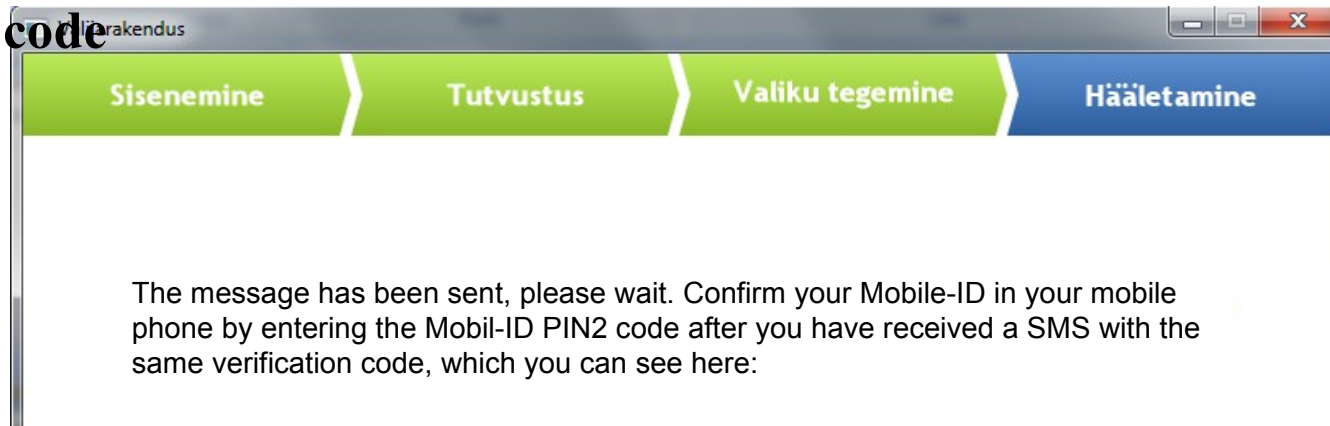
Tagasi

Hääletan

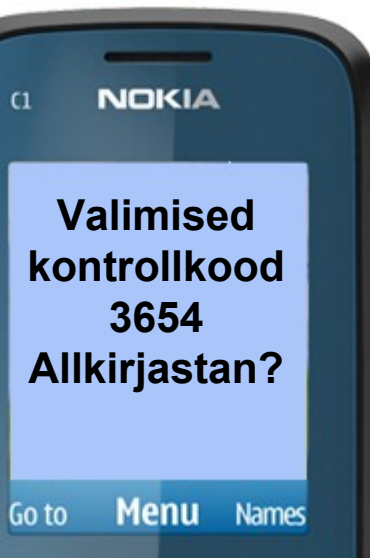
Confirmation (mobile-ID)



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



3654



Vote received



Valijarakendus

Sisenemine > Tutvustus > Valiku tegemine > Hääletamine

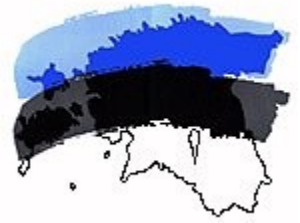
Your vote has been received

You can change your vote while the electronic voting is open (24 Feb to 2 March) or by voting in paper on pre-voting days at a polling station (28 Feb to 2 March).
On election-day (6 March) you can't change your vote!
If you have casted several electronic votes only the last vote will be taken into account. If you have voted on paper at a polling station your electronic vote is withdrawn.
On the 6th of March there will be a notification on the paper voters list in your local polling station that you have voted electronically.

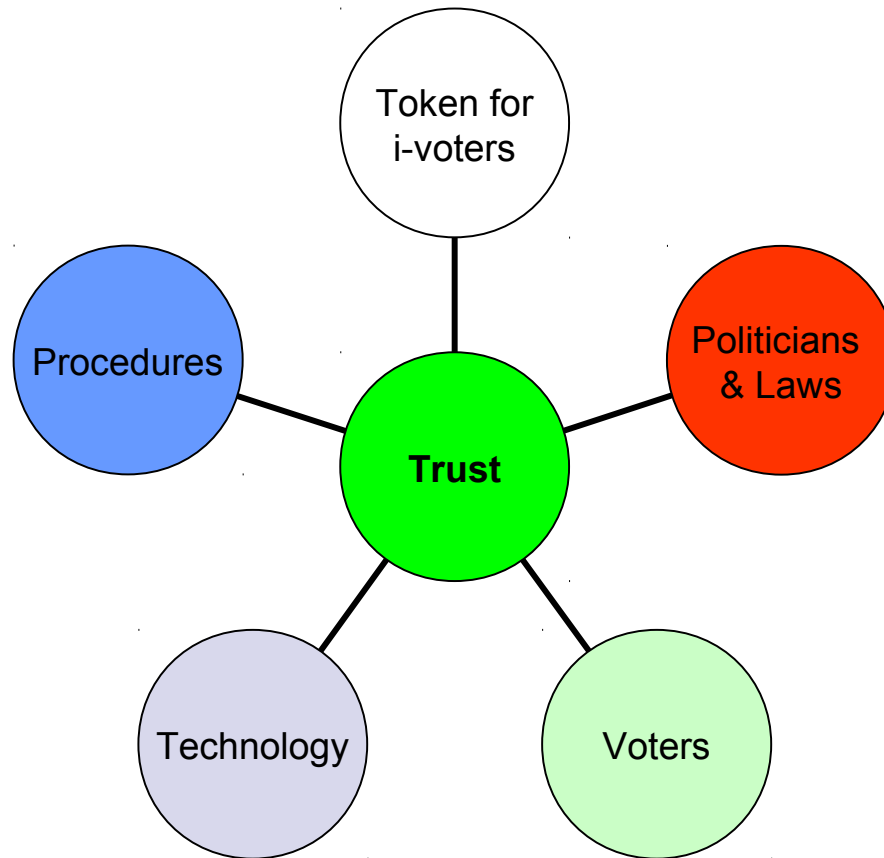
Please close the application. For enhanced security please remove the ID card from the reader!

Valmis

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

Voting



(1): ID-card authentication



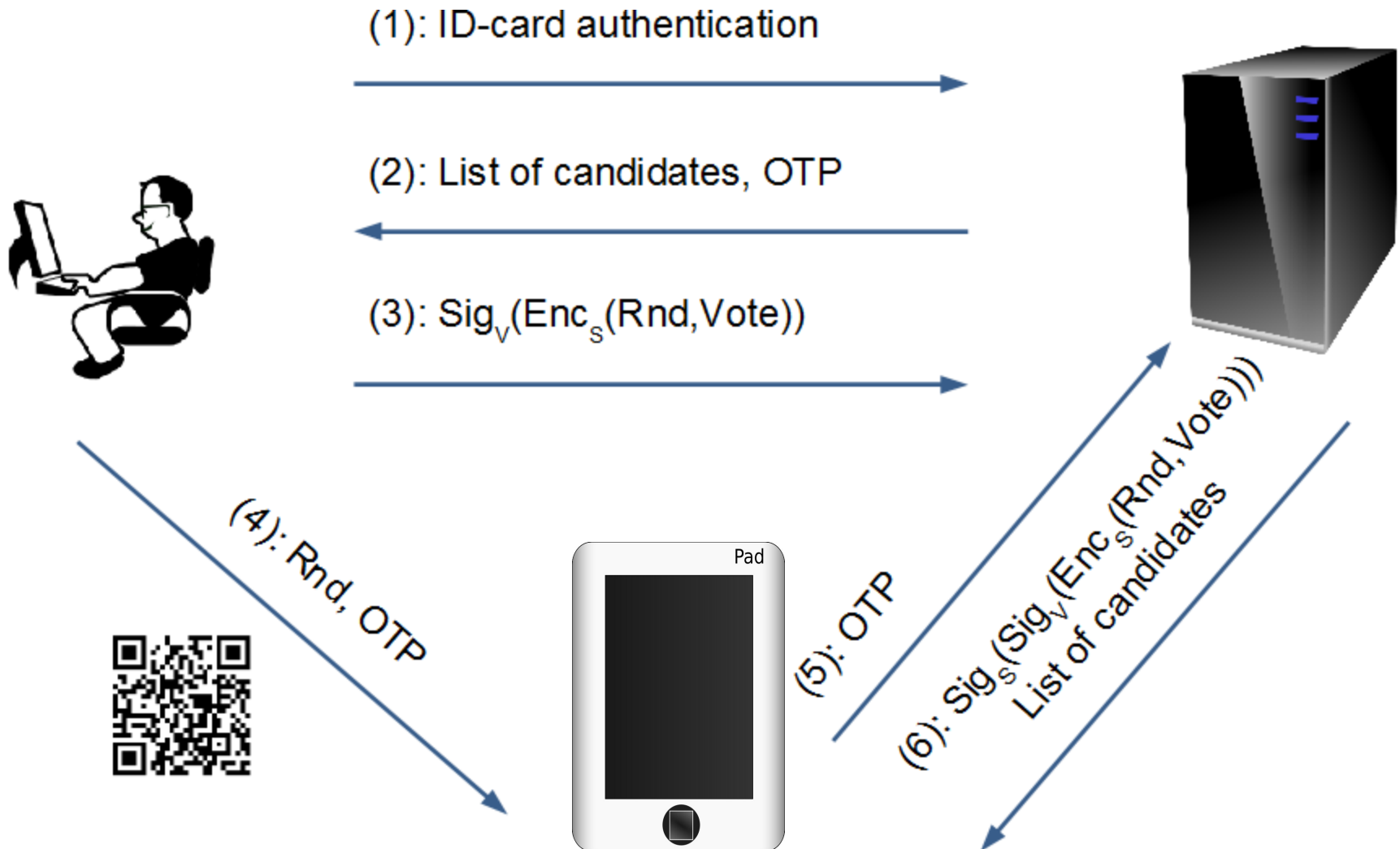
(2): List of candidates



(3): $\text{Sig}_V(\text{Enc}_S(\text{Rnd}, \text{Vote}))$



Voting with verification





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

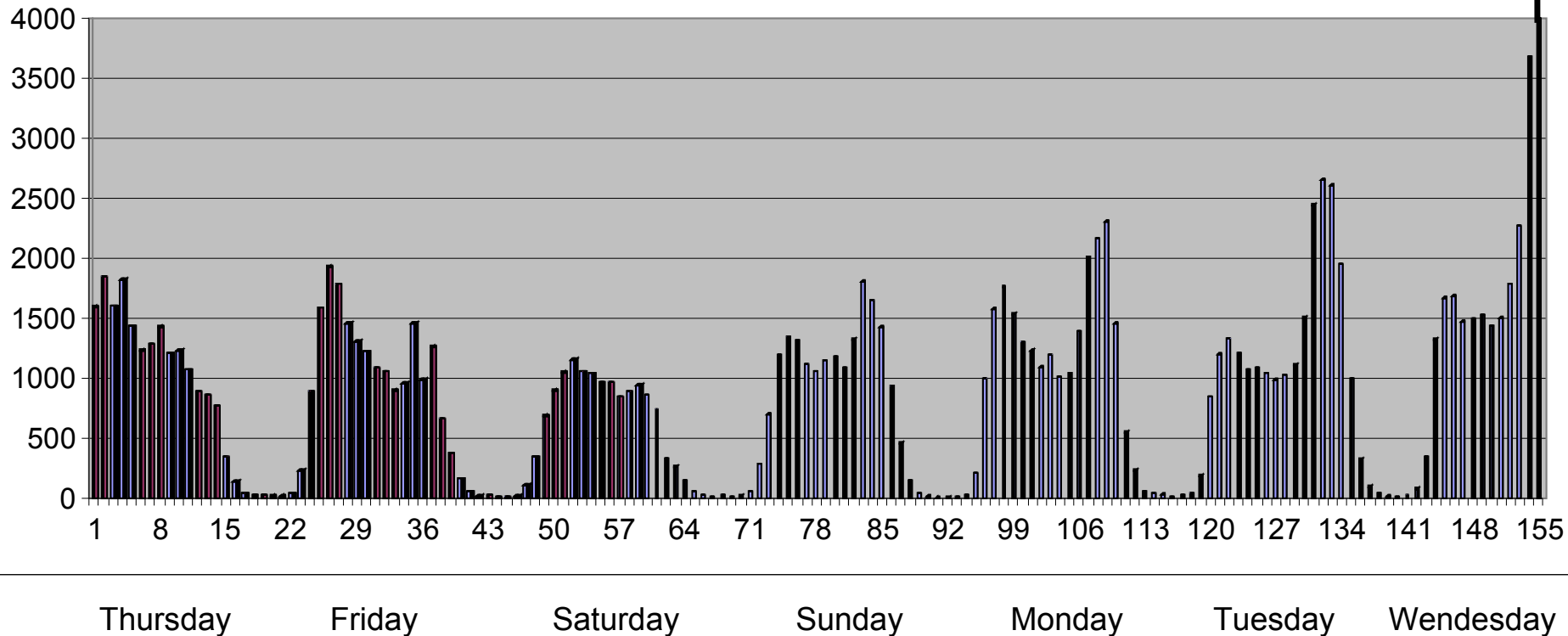
Statistics 2005..2011



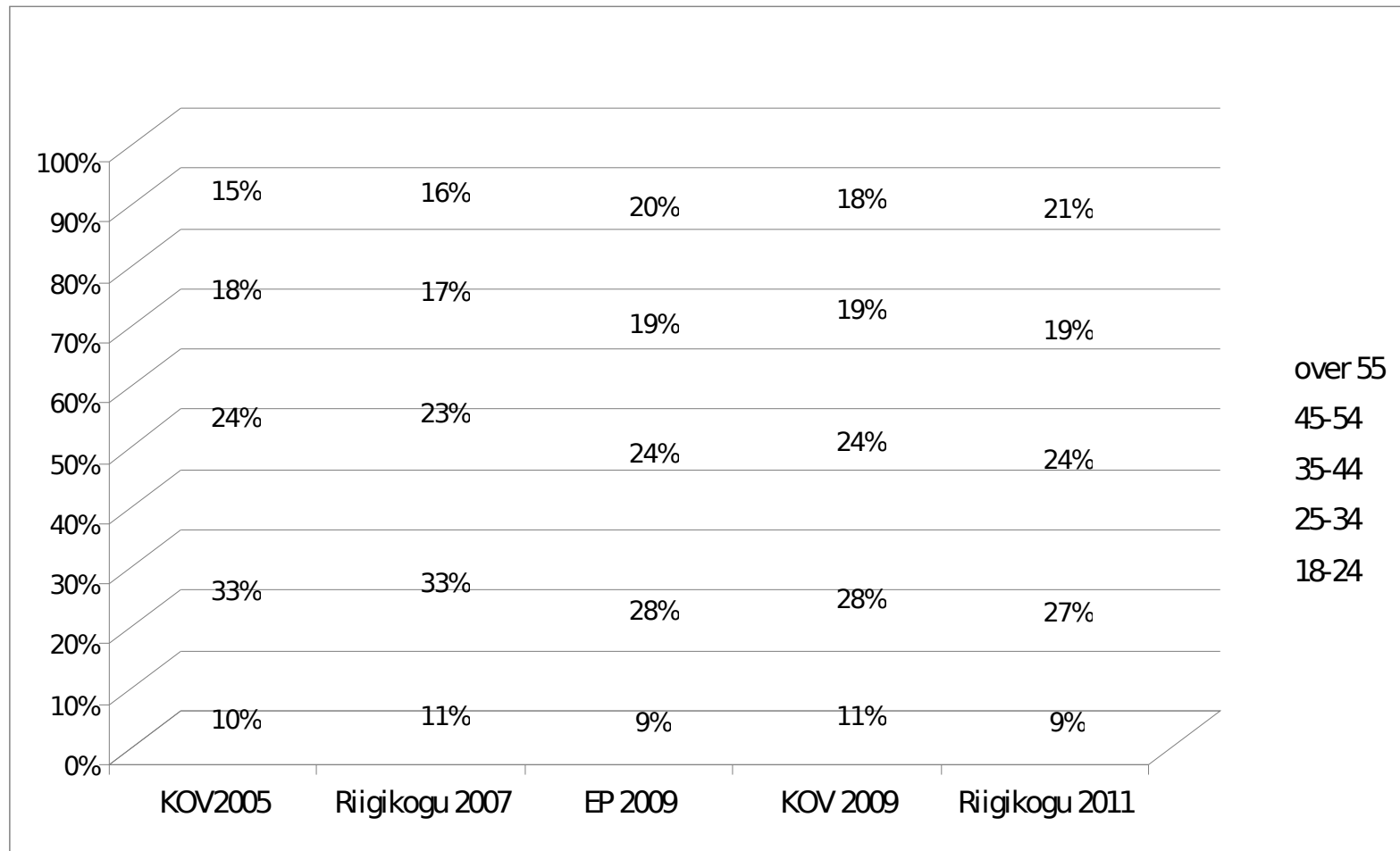
Votes per hour, 2011



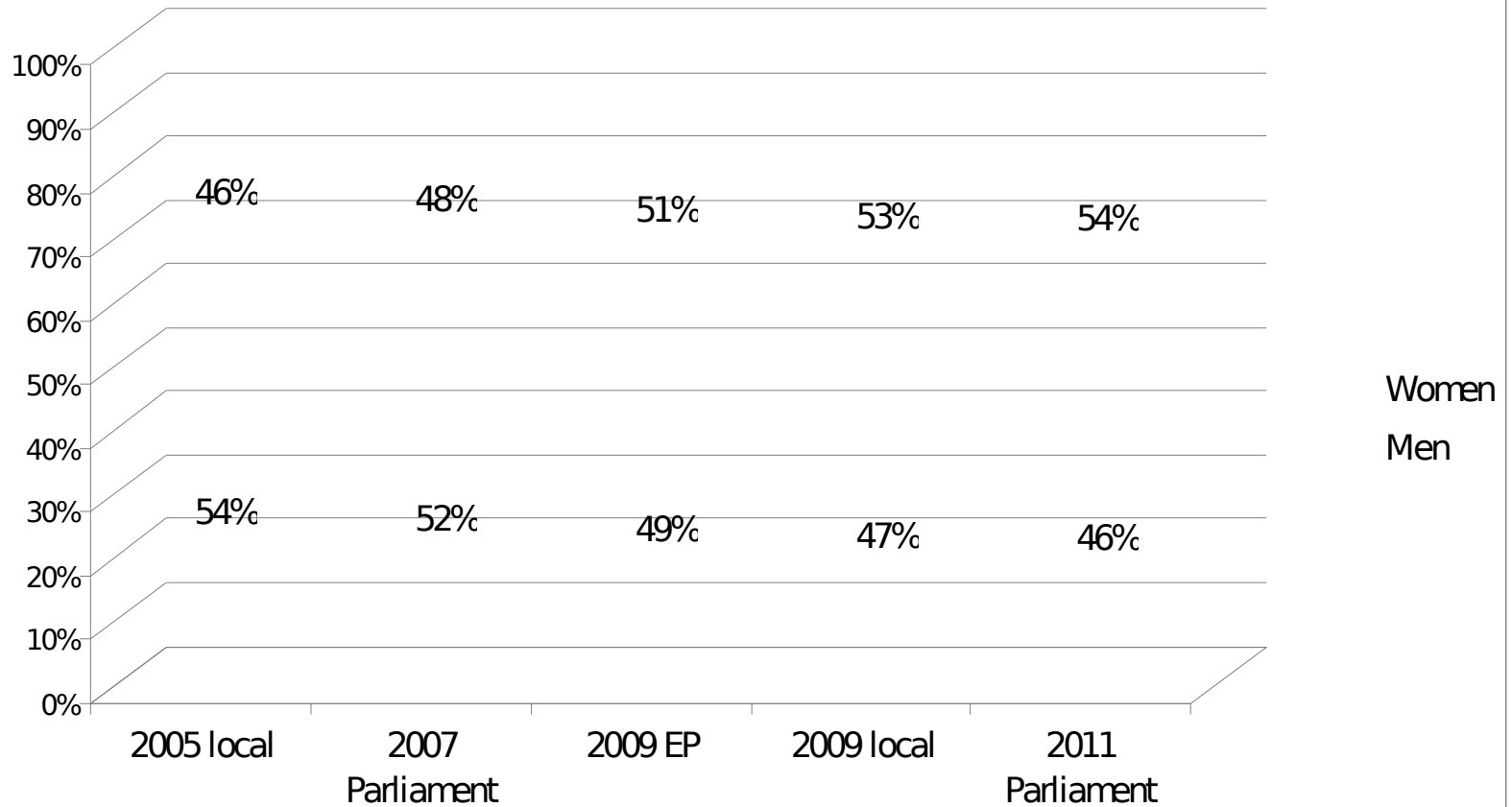
7081+98



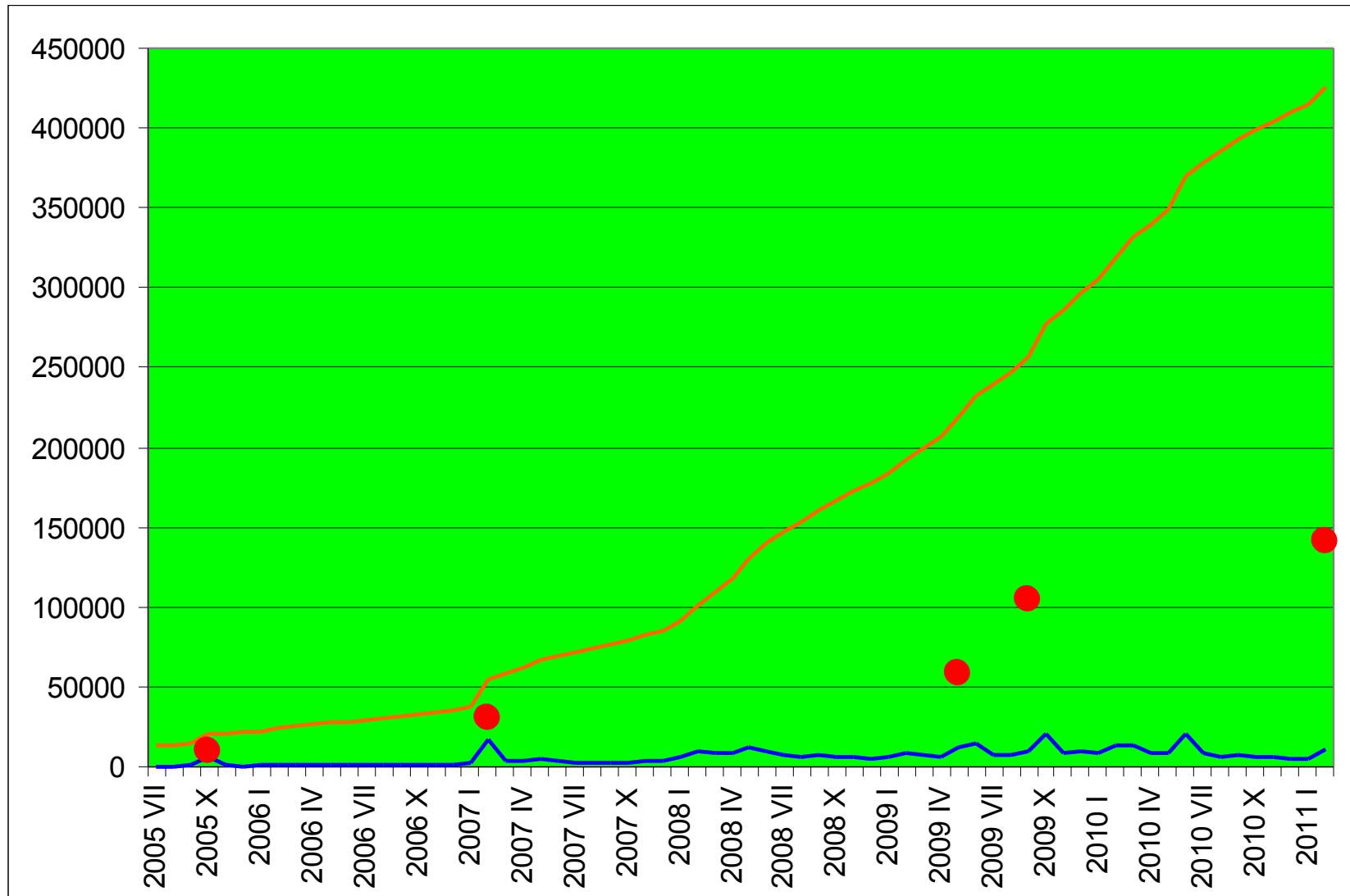
How old is the I-voter?



Sexual equality?



ID-card usage vs. I-voting

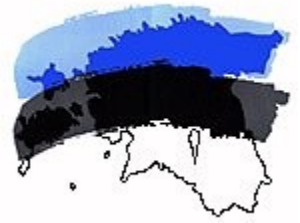




Lessons learned

- 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