

I-hääletamise arengutest



Tarvi Martens
juhataja

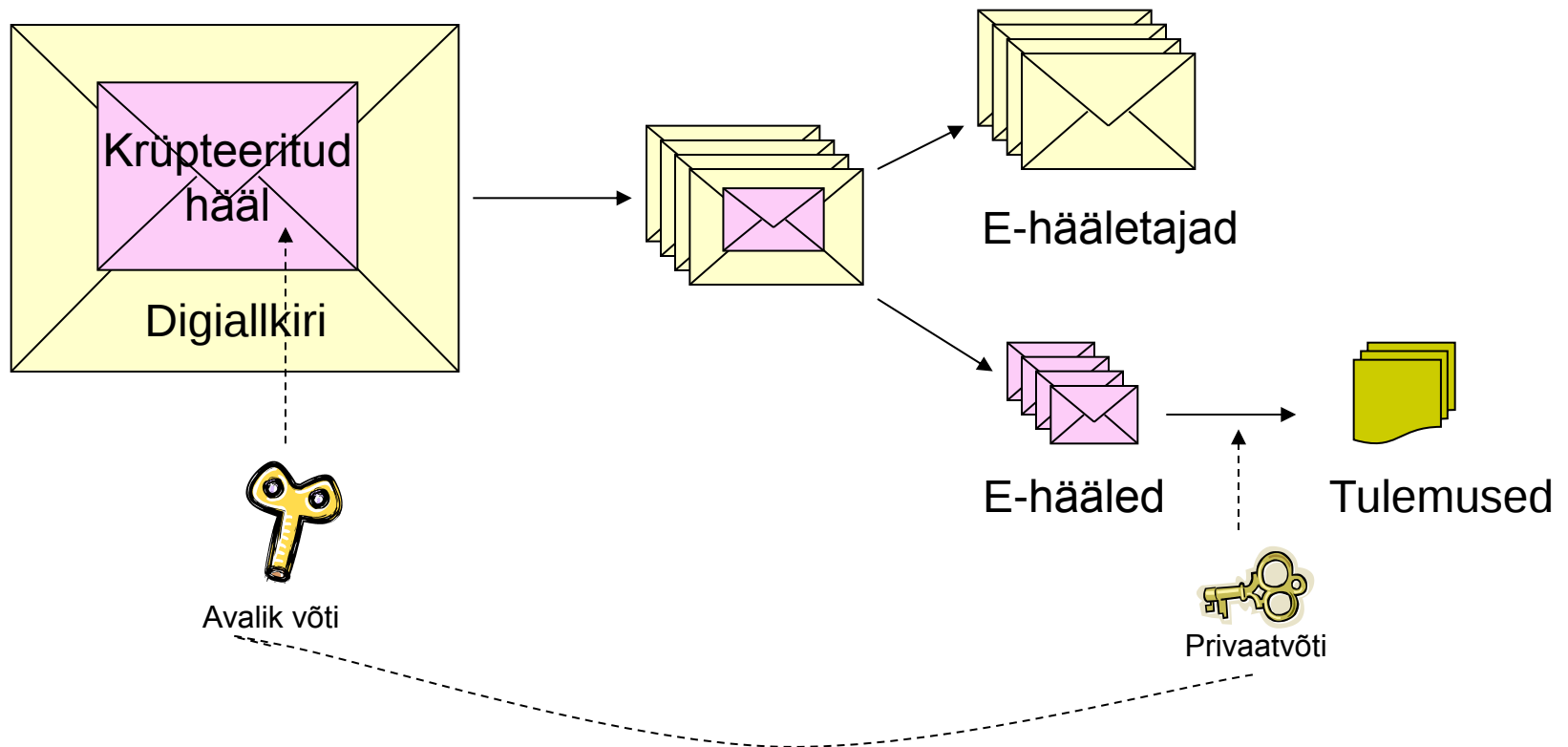
Elektroonilise Hääletamise
Komisjon

Fakte



- Juhtus juba kuuendat korda (2005-ndast)
- Kolmandat korda KOV valimistel
- **133808 e-hääletajat**
 - 28% rohkem kui KOV 2009
 - 5% vähem kui RK 2011
- Mida uut:
 - Hääle kohalejõudmise kontrollimine
 - Avalik lähtekood
 - Kõik filmilood on avalikult YouTube's

Ümbrikuskeem



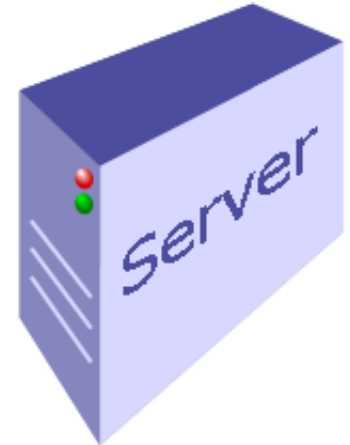
Hääle kontrollimine



(1): autentimine

(2): Kandidaatide nimekiri, OTP

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



(4): Rnd_V, OTP



(5): OTP

(6): $\text{Enc}_S(\text{Rnd}_V, \text{Vote}_V)$
Kandidaatide nimekiri



valikud



hää



juhuarv

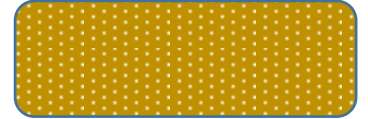
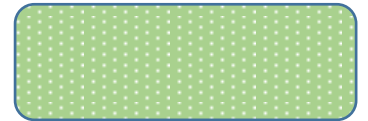
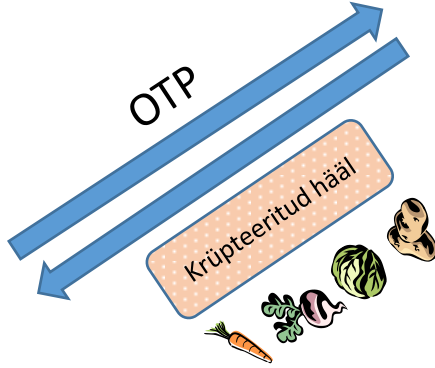
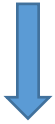


Krüpteeritud
hää
digiallkiri



OTP







Läbipaistvuse põhimõte

- Kõik süsteemi komponendid peavad olema auditeeritavad
- „Musti kaste“ ei sallita
 - Suletud autentimissüsteemid on „out“
 - Ilma lähtekoodita komponente ei kasutata

Tarkvara lähtekood avalik!



- <https://github.com/vvk-ehk/>
 - Serveripoolne lähtekood (3 serverit)
 - Kontrollrakendus Androidile
- Kliendipoolne tarkvara lähtekood endiselt salajane:
 - teeks liiga lihtsaks võlts-rakenduse loomise
 - avaliku lähtekoodiga kontrollrakendus avastab kliendi valekäitumise nii-kui-nii.



Haldusprotseduurid

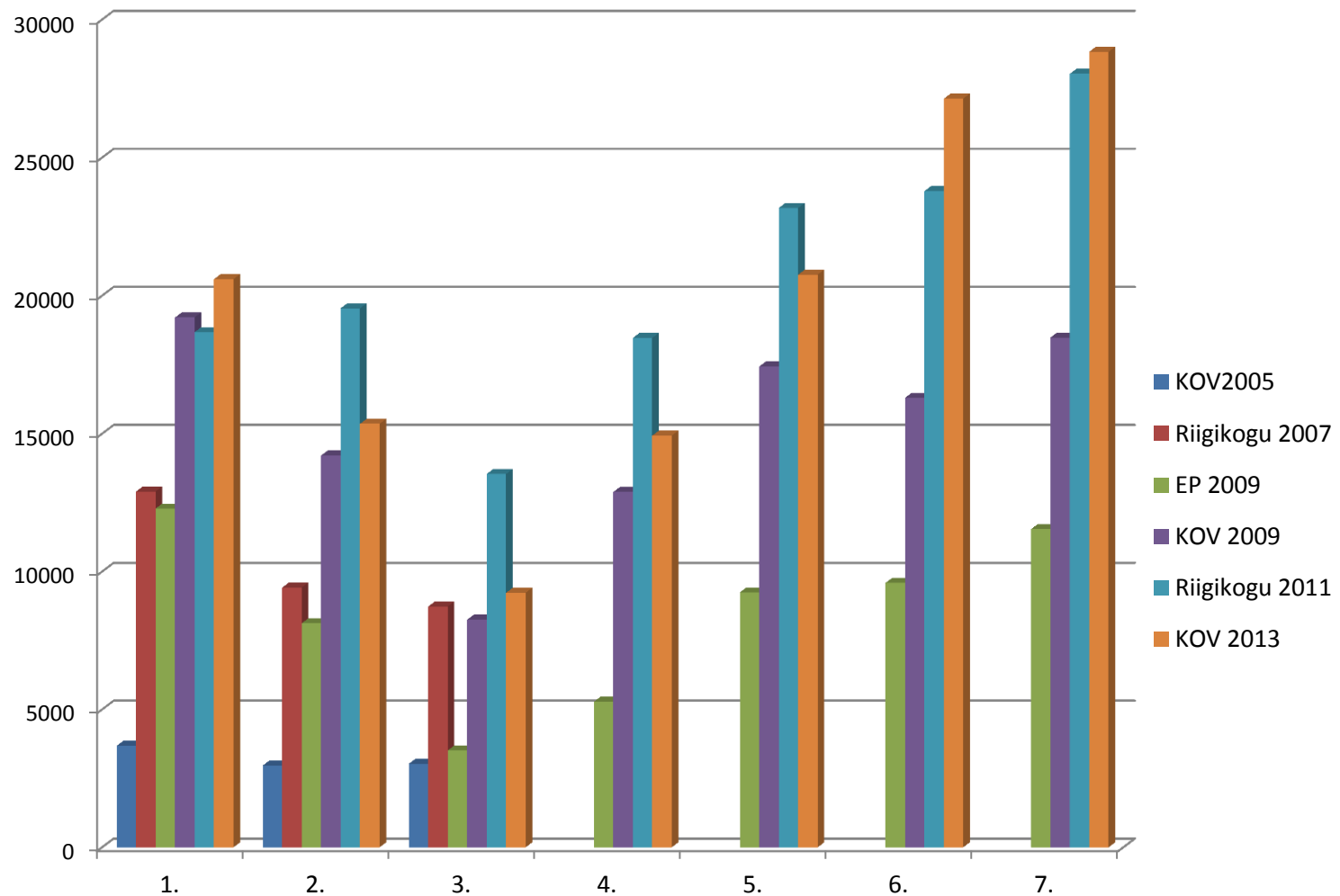
- Kõik on viimseni dokumenteeritud
 - Ja avalik!
 - Kiirkursused audiitoritele ja vaatlejatele
 - Kõik turvatundlikud protseduurid:
 - Logitakse
 - Vaadeldakse ja auditeeritakse
 - Filmitakse
- (<http://www.youtube.com/channel/UCTv2y5BP0o-ZSVdTg0CDIbQ>)



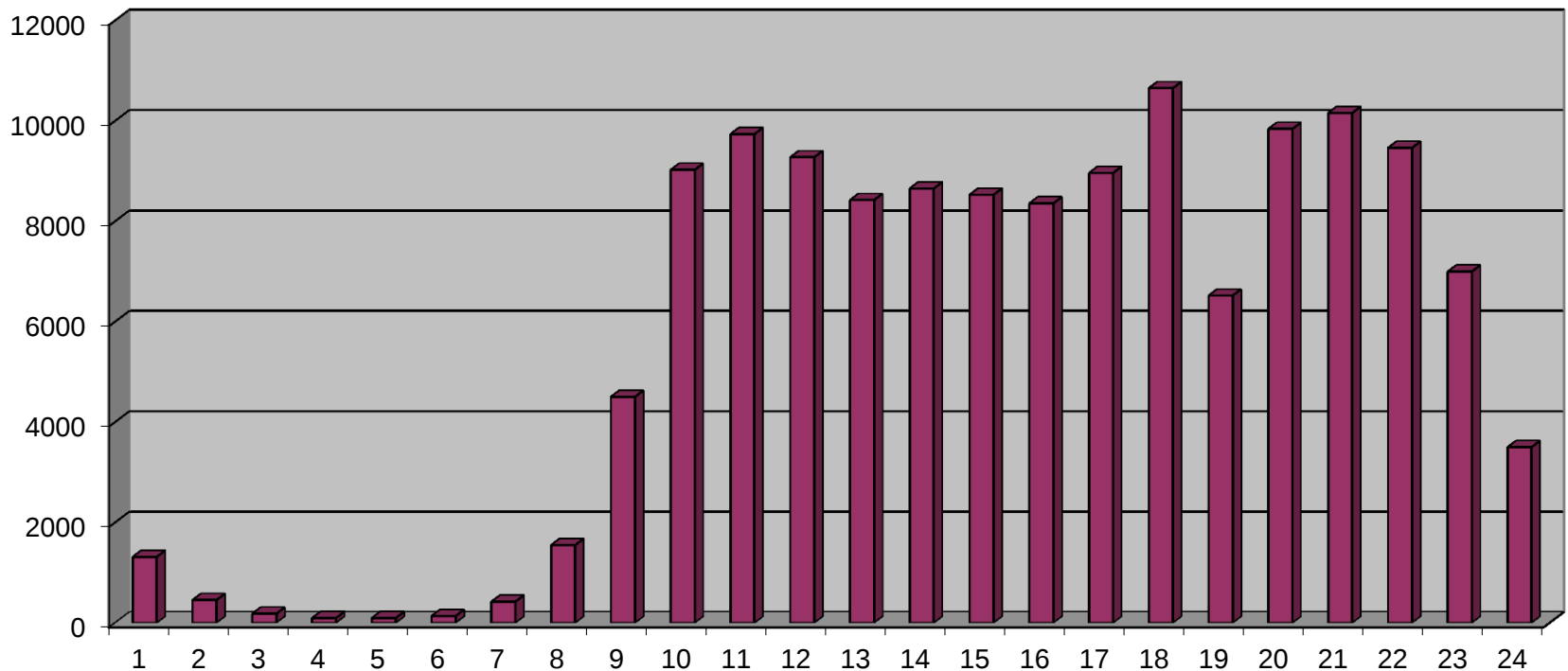
Vaatamist talveõhtuteks

- 1.10 – operatsioonisüsteemide installeerimine
- 2.10 – võtmepaari genereerimine
- 4.10 – süsteemi seadistamine ja prooviläbimine
- 8.10 – süsteemi ülespanek majutuskohta
- 10.10 – e-hääletamise algus!
- 10.10..16.10 – valijate nimekirjade uuendamine, süsteemi varundamine
- 16.10 – e-hääletamise lõpp!
- 17.10 – e-hääletanute nimekirja koostamine
- 20.10 – e-häälte kokkulugemine

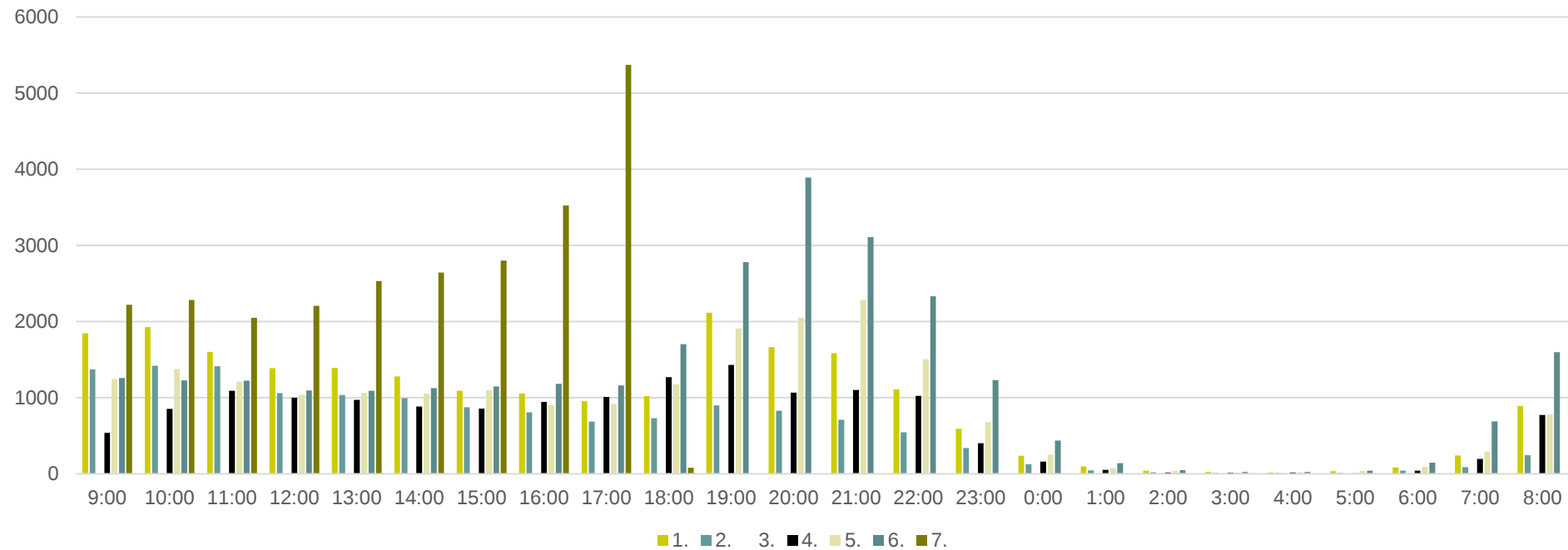
Hääletamine päevade lõikes



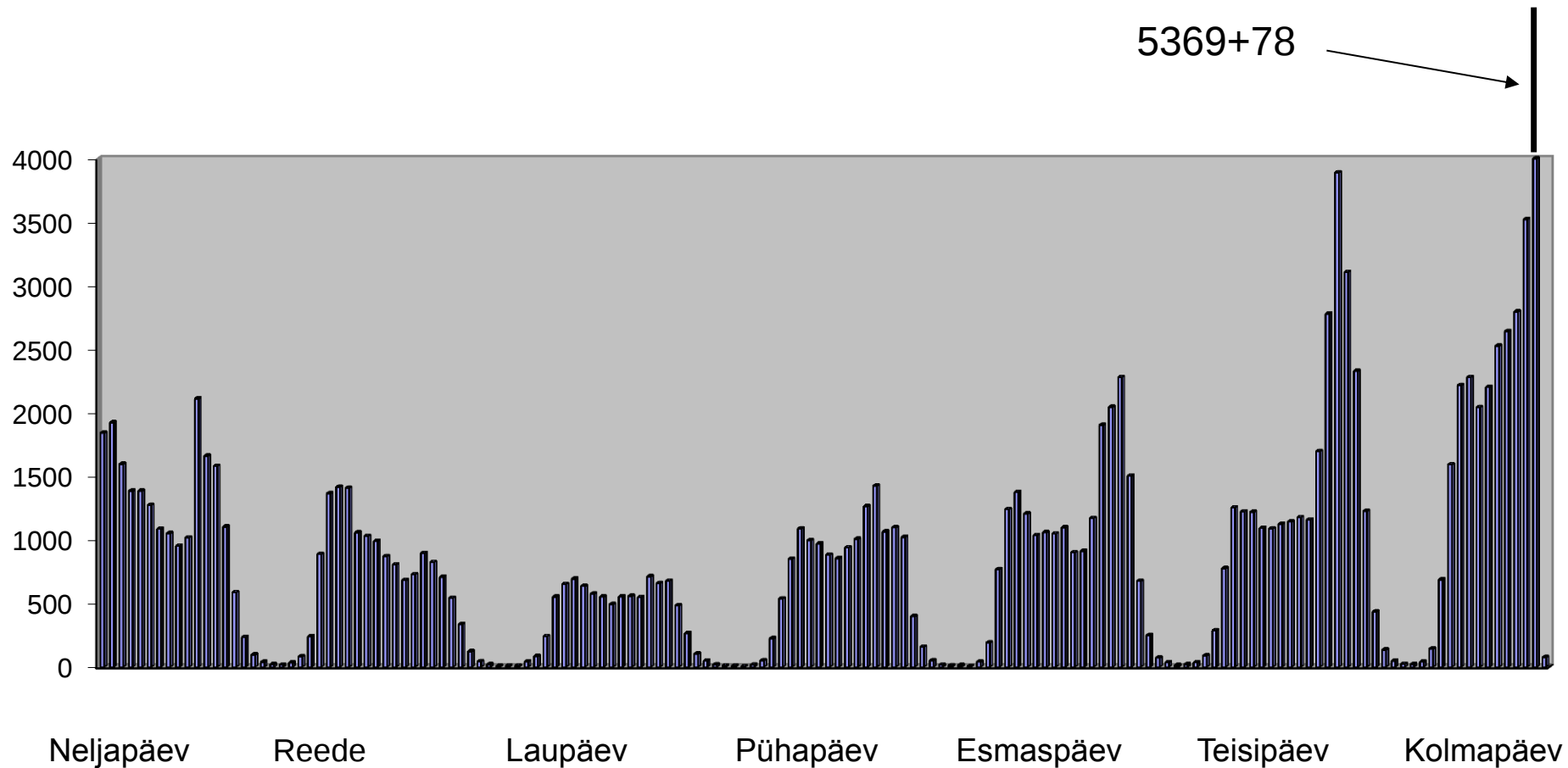
Jagunevus tundide lõikes



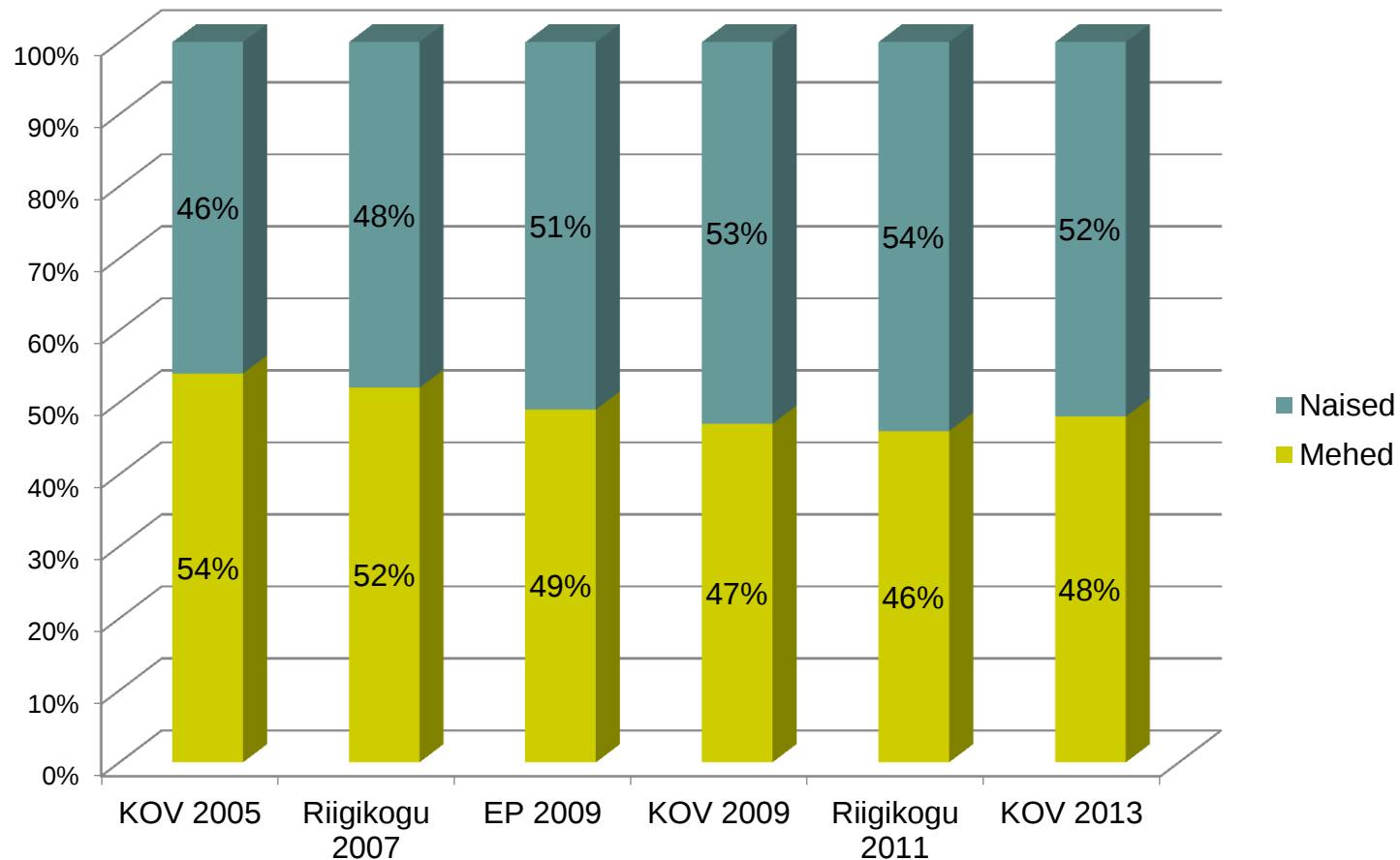
Tundide lõikes...



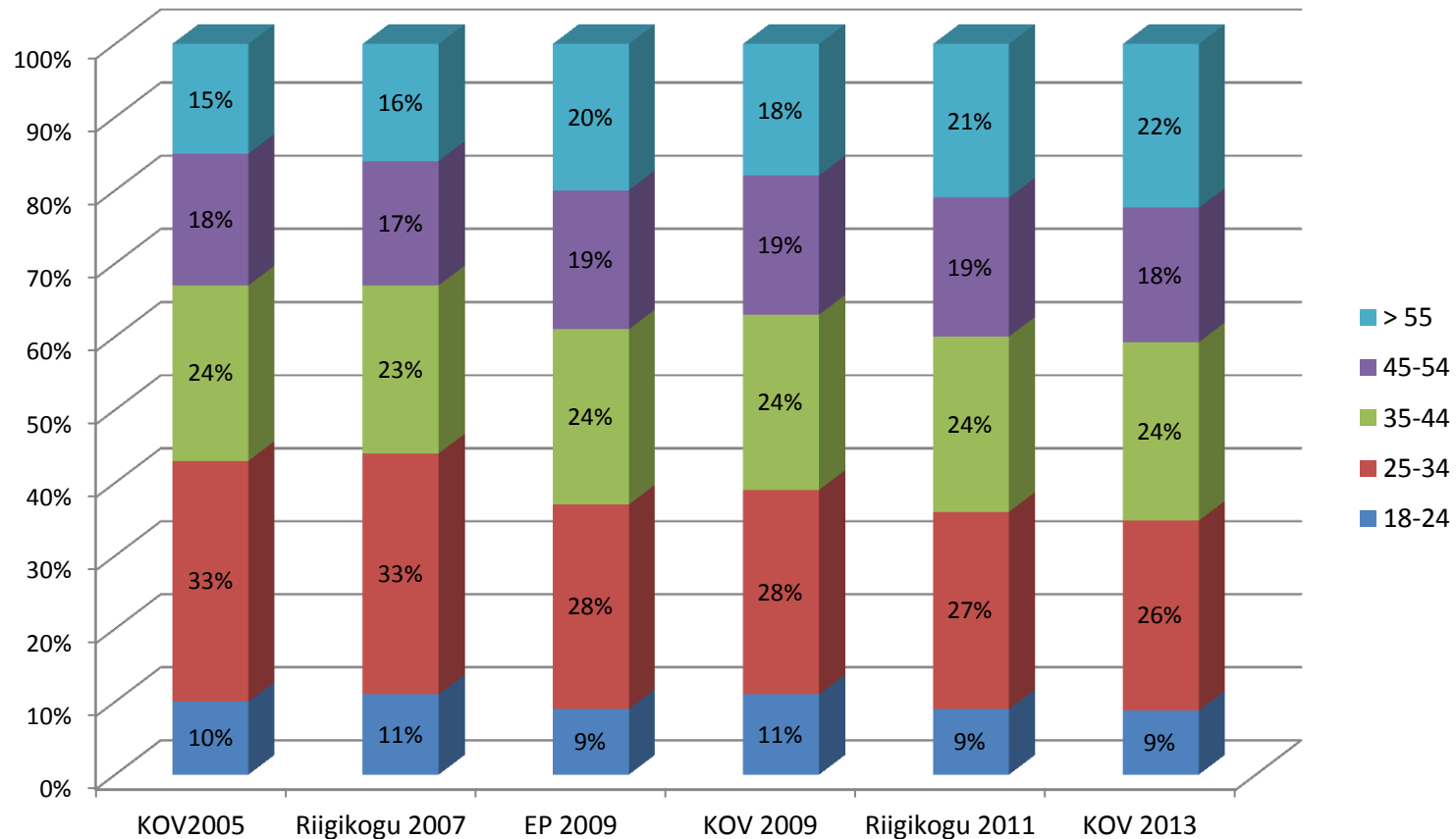
Kõik päevad



Võrdõiguslikkus?



E-hääletamine ainult noortele?





Muid numbreid

- Kontrollitud e-hääli: 4696 (3,43%)
- Kasutatud eID:
 - Mobiil-ID 8,59% (4x kasv vs 2011)
 - ID-kaart 90,15%
 - Digi-ID 1,26%
- Kasutatud arvuti:
 - Windows 93,80%
 - MacOSX 5,37% (2x kasv vs 2011)
 - Linux 0,83%
- Kiireim minut: 134 häält/minutis (17:40, kolmapäev)
- Klienditugi:
 - 266 vastatud e-kirja (RK2011: 532)
 - 701 vastatud kõnet (RK2011: 886)

Hääletame maikuus 2014 edasi



www.valimised.ee

tarvi@sk.ee