

Nutiseadmete? Brauserisse?

Sven Heiberg

sven@ivotingcentre.ee

Hääletamine brauseris, 2007

Teie brauser kas ei toeta ActiveX komponentide kasutamist
või on komponentide kävitamine keelatud.

Operatsioonisüsteemi Microsoft Windows kasutajad saavad
hääletamiseks kasutada valijarakenduse EXE-versiooni:

Valijarakenduse EXE-versioon Windowsi jaoks (1,9 MB)

Vabariigi Valimiskomisjon

Hääletamine brauserita, 2009 - ...

Sisenemine Tutvustus **Valiku tegemine** Hääletamine

Siillased
101 HARILIK SIIL
102 KAELUSSIIL

Mutlased
103 MUTT

Karihiirlased
104 METS-KARIHIIR
105 LAANE-KARIHIIR
106 VÄIKE-KARIHIIR
107 KÄÄBUS-KARIHIIR
108 VESIMUTT

Karulased
109 PRUUNKARU

Nahkhiirlased
110 TIIGILENDLANE
111 VELENDLANE
112 BRANDTI LENDLANE
113 HABELENDLANE
114 NATTERERI LENDLANE
... . .

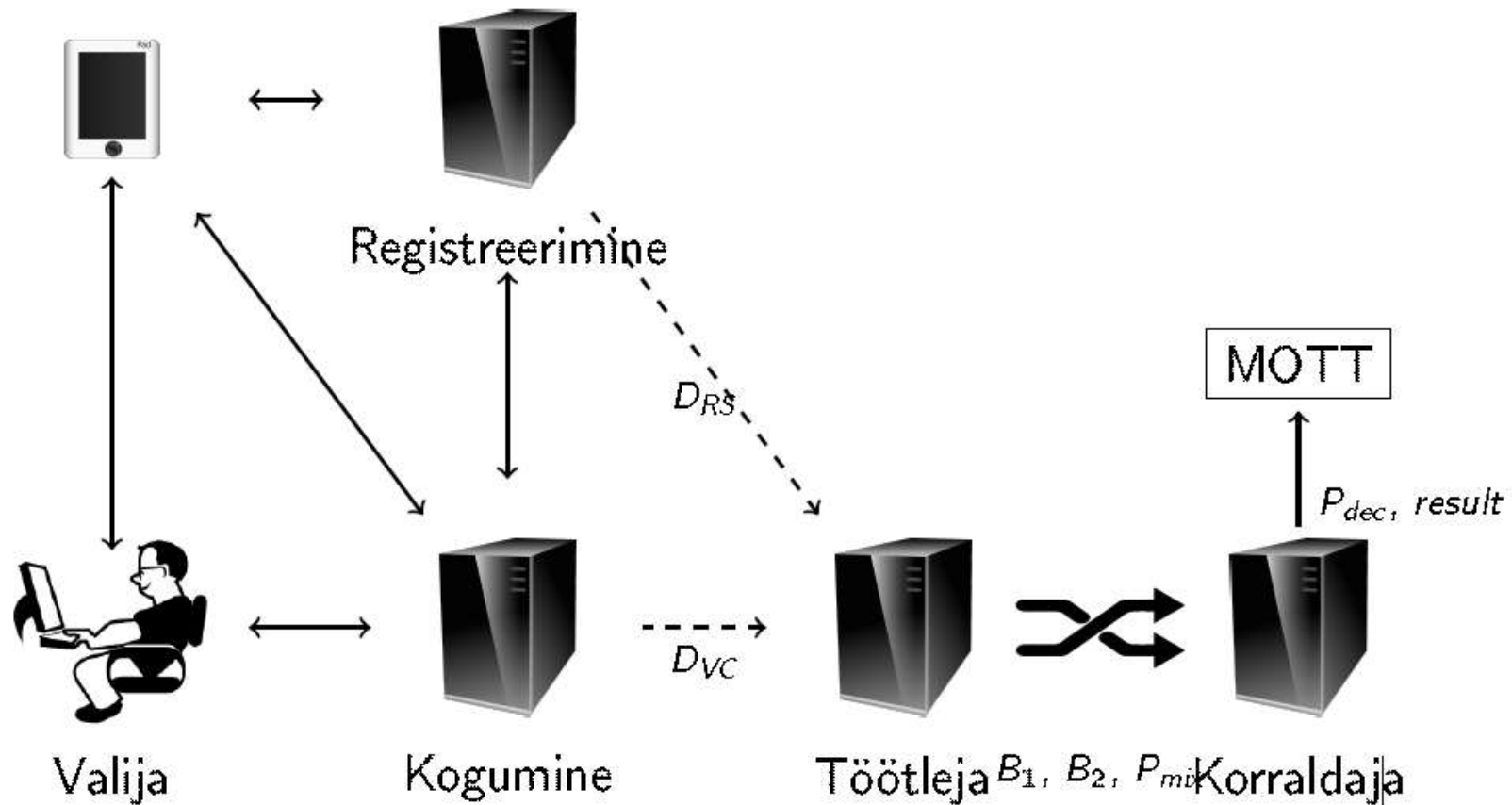
Kelle valite Riigikogusse?
Klõpsake soovitud kandidaadi nimele.

Teie valimisringkond:
Põlislaas - Valimisringkond nr 2

Minu valik on:
kandidaat nr 109
PRUUNKARU
Karulased

Katkestan **Valin**

Hääletamisprotokoll



Mida peab valijarakendus oskama?

- TLS ühenduse loomine ja usaldusväärseuse kontrollimine
- eID kasutamine (ID kaart, mID)
- Valiku krüpteerimine (juhuslikkus, ElGamal)
- Valiku signeerimine (SHA256, BDOC, XML, ZIP)
- Hääle verifitseerimine
 - RSA/ECC signatuuri verifitseerimine
 - OCSP vastuse verifitseerimine
 - PKIX ajatempli verifitseerimine
- QR-koodi genereerimine
- Samuti oluline evitamise turvalisus ja lihtsus

Nutiseadmed valimisel



App valijarakendusena?

- Kõik teemad on lahendatavad kui unustame ID-kaardi
- OS versioonide ühildamatuse tõttu tuleb süsteemsed teegid unustada (TLS ja muu krüpto)
- iOS ja Android vahel koodibaasi jagamine küsitav
- Evitamise turvalisus ja lihtsus?
 - Hääletamine algab marketist
 - iOS tsükel tüslik
 - Android võimaldab avatud lähtekoodi korral korratavaid builde
- Kuidas kontrollime?
 - Sama mehhanism, aga infovahetus? Platvormide sõltumatus?

Häätamine brauseris, 2014 - ...

SMARTMATIC GOUVERNANCE | **MAIPÚ** | **Presupuesto Participativo MAIPÚ 2015** | **TU BARRIO GANA**

AUTENTICACIÓN | INTRODUCCIÓN | BARRIOS | **PROYECTOS** | CONFIRMAR ?

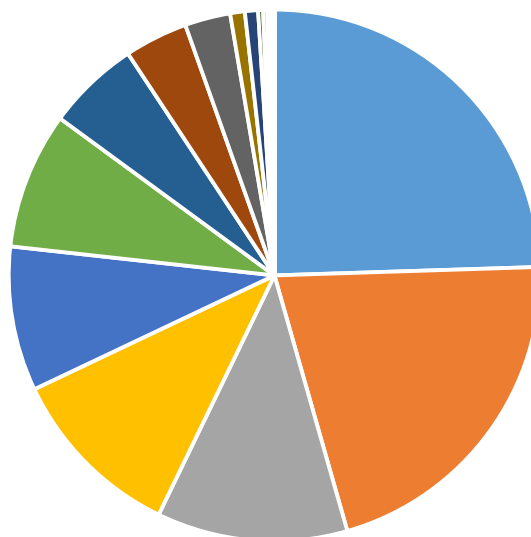
Proyectos del barrio: Los Bosquinos J
Seleccione el proyecto de su preferencia (Vote por 1)

J1	Cierres Perimetrales Club Deportivo Social y Cultural Hernán Díaz Arrieta	<input type="checkbox"/>
J2	Cierres Perimetrales JJVV Los Bosquinos	<input type="checkbox"/>
J3	Instalación de Máquinas de ejercicio con pérgola JJVV Bosques del Sur	<input checked="" type="checkbox"/>
J4	Instalación de Máquinas de ejercicio con pérgola JJVV Bosques del Sur	<input type="checkbox"/>
J5	Instalación de Máquinas de ejercicio con pérgola JJVV Hernán Díaz Arrieta Etapa II y III	<input type="checkbox"/>
J6	Instalación de Máquinas de ejercicio con pérgola JJVV Los Bosquinos III	<input type="checkbox"/>
J7	Juegos Infantiles: Balancín 4 niños, tobogán, columpio, sistema modular JJVV Hernán Díaz Arrieta Etapa I	<input type="checkbox"/>

[REGRESAR](#) [CONTINUAR](#)

Brauserite jaotus 2018 ühtedel valimistel

Sales



- | | | |
|---------------------|------------------------------|-------------------------|
| ■ Mobile Safari | ■ Chrome | ■ Chrome Mobile |
| ■ Facebook | ■ Samsung Internet | ■ IE |
| ■ Edge | ■ Firefox | ■ Safari |
| ■ Chrome Mobile iOS | ■ Opera | ■ Chrome Mobile WebView |
| ■ Firefox Mobile | ■ Mobile Safari UI/WKWebView | ■ Opera Mobile |
| ■ Edge Mobile | ■ Vivaldi | ■ IE Mobile |
| ■ Chromium | ■ Firefox iOS | ■ Pale Moon |
| ■ Maxthon | ■ Yandex Browser | ■ Android |

Brauser valijarakendusena? Eestis?

- Taaskord teemad lahendatavad, kui unustame ID-kaardi
 - ID-kaardi toetamine siiski võimalik
- Siiski probleemid krüptoga
 - Usaldusväärsed teegid praktiliselt puuduvad
 - Kvaliteetne juhuslikkus?
 - XML/BDOC JavaScriptis?
 - Signatuuri verifitseerimine
 - OCSP vastuse verifitseerimine
 - PKIX ajatempli verifitseerimine
- JavaScript või TypeScript?
- Evitamise turvalisus ja lihtsus
 - Koodi terviklus?

Järeldused