Elektroonilise hääletamise protokollistik III: Kontrollprotokoll

Dokumendi liik

Redaktsioon: 1.4

24.01.2015

16 lk

Kuupäev	Nr	Kirjeldus	Autor
01.12.2012	0.1	Dokumendi algversioon	Cybernetica AS (Sven Heiberg)
15.01.2013	1.0	Kontrollprotokolli täpsustused • HTTPS autentimine • Digitaalallkirja kontrolli eemaldamine • Andmestruktuuride täpsustamine	Cybernetica AS (Sven Heiberg)
13.09.2013	1.1	Valija isikuandmete eemaldamine protokollist	Cybernetica AS (Sven Heiberg)
18.09.2013	1.2	Seadistuste laadimine	Cybernetica AS (Sven Heiberg)
18.04.2013	1.3	Täpsustused seadistustes	Cybernetica AS (Sven Heiberg)
24.01.2013	1.4	JSON seadistuste definitsioon	Cybernetica AS (Sven Heiberg)

Annotatsioon

Dokument spetsifitseerib valijarakenduse, kontrollrakenduse ning kesksüsteemi vahelise protokolli elektroonilise hääle kontrollimiseks.

Sisukord

1 Sissejuhatus

1.1 Kontrollprotokolli skoop

Kontrollprotokoll spetsifitseerib kontrollrakenduse ja valijarakenduse ning elektroonilise hääletamise kesksüsteemi vahelise päringuvahetuse, mille käigus kontrollitakse valija tahteavalduse korrektset jõudmist elektroonilise hääletamise kesksüsteemi.

1.1.1 Üldkirjelduses defineeritud andmestruktuurid

Dokument viitab mitmetele andmestruktuuridele, mis on defineeritud protokollistiku üldkirjelduses [EHI]:

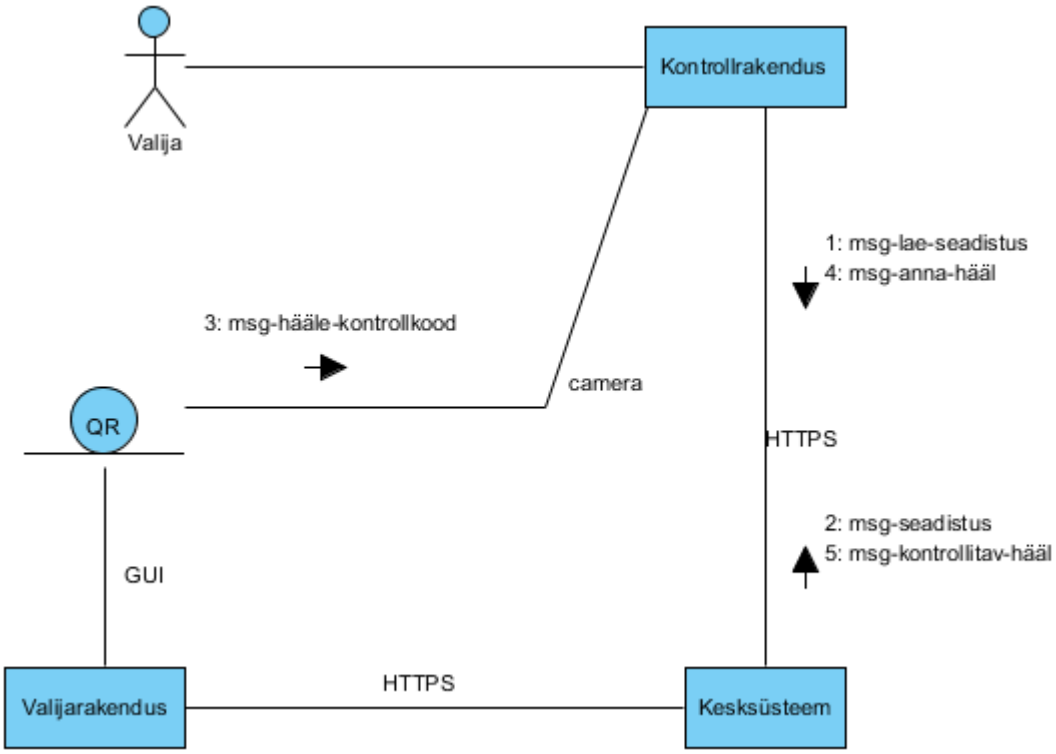
```
valikute-nimekiri

valimised

valimise-identifikaator

versiooninumber

kontrollkood

krüpteeritud-hääl
```

1.2 Viited

1. [EHI] – Elektroonilise hääletamise protokollistik I: Üldkirjeldus.
2. [HTTPS] – HTTP Over TLS. RFC2818
3. [QR] - QR code, http://www.qrcode.com/en/index.html

2 Sõnumivahetus

Kontrollprotokolli sõnumivahetus on kirjeldatud joonistusel 1.



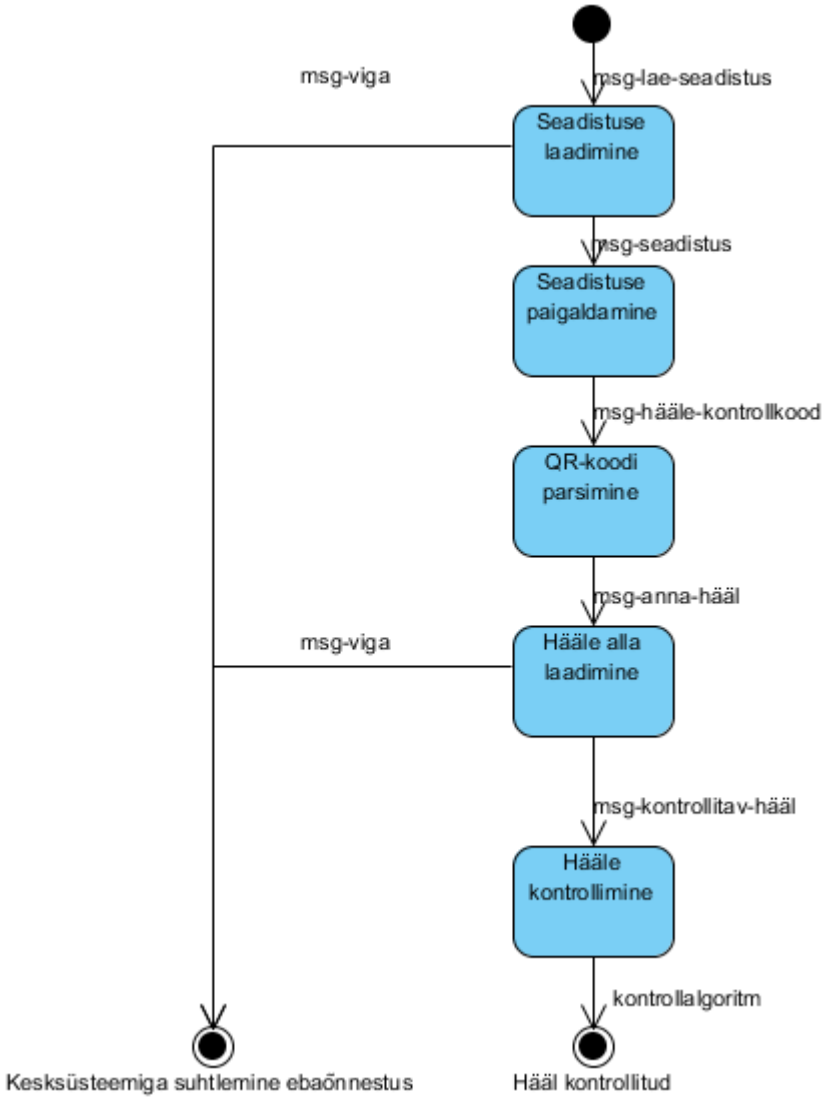
Joonistus 1: Kontrollprotokoll

Protokoll järgneb hääletamisele valijarakendusega:

1. Kontrollrakendus saadab kesksüsteemile sõnumi `msg-lae-seadistus`.
   - Kontrollrakendus pöördub kesksüsteemi URLile ning verifitseerib kesksüsteemi sertifikaati.
2. Kesksüsteem saadab kontrollrakendusele sõnumi `msg-seadistus`.
3. Kontrollrakendus pildistab valijarakenduse graafilist sõnumit `msg-hääle-kontrollkood`.
   - Sõnum sisaldab valimiste häälte krüpteerimiseks kasutatud juhuarve ning valija häälele viitavat unikaalset identifikaatorit.
4. Kontrollrakendus saadab kesksüsteemile sõnumi `msg-anna-hääl`.
   - Sõnum sisaldab häälele viitavat unikaalset identifikaatorit.
5. Kesksüsteem saadab kontrollrakendusele sõnumi `msg-kontrollitav-hääl`.
   - Sõnumi vastuseks on identifikaatori poolt viidatavat häält sisaldav konteiner koos vastava valikute nimekirjaga või veateade, kui häält ei eksisteeri või hääle kontrollimiseks olnud aeg on möödunud.

Seadistusi jagavad ja hääli väljastavad kesksüsteemi komponendid võivad paikneda erinevates masinates, nende sertifikaadid pärinevad ühtsest hierarhiast.

Kui joonistusel 1 on kujutatud üks instants kontrollprotokollist, siis joonistusel 2 on esitatud kontrollprotokolli olekumasin, mis defineerib võimalikud sõnumivahetusstsenaariumid kontrollprotokollis.



Joonistus 2: Kontrollprotokolli olekumasin

3 Protokolli sõnumid

3.1 Sõnumi struktuur

Rakendustaseme kontrollprotokoll kasutab sõnumivahetuseks HTTPS protokolli [HTTPS]. Kontrollrakenduse sõnumid kesksüsteemile esitatakse POST-päringutena etteantud URLile. Kesksüsteemi vastussõnumid on text/plain tüüpi dokumendid, mille ülesehitus on kolmeosaline. Sõnum sisaldab protokolli versiooninumbrit, oleku koodi ning protokolli sammust sõltuvat teadet.

```
sõnum = versiooninumber LF oleku-kood LF teade

; välja teade struktuur sõltub protokolli sammust

oleku-kood = olek-ok | olek-viga

olek-ok = 0

olek-viga = 1
```

Oleku koode kasutatakse järgmises tähenduses:

- `olek-ok` – operatsioon õnnestus, teate tõlgendamine sõltub protokolli sammust;
- `olek-viga` – viga kesksüsteemiga suhtlemisel, täpsem info vea kirjelduses.

3.2 Kontrollrakenduse sõnum `msg-lae-seadistus`

Kontrollrakendus teeb seadistuste – rakenduse tekstid, fondid, värvid, avalik võti, valimiste identifikaatorid, URLid – laadimiseks kesksüsteemi seadistus-URLile GET päringu. Päringu tulemusena luuakse TLS-ühendus, kusjuures kontrollrakendus verifitseerib serveri sertifikaati.

Võimalikud vastussõnumid:

- `msg-seadistus` – kontrollrakenduse seadistused.
- HTTP protokolli veateade

3.3 Kontrollrakenduse sõnum `msg-seadistus`

Sõnum saadetakse vastuseks kontrollrakenduse sõnumile `msg-lae-seadistus`.

```
msg-seadistus = BLOB

; vaata täpset kirjeldust peatükist 5.
```

3.4 Valijarakenduse sõnum `msg-hääle-kontrollkood`

Selle sõnumiga saab kontrollrakendus valijarakenduselt teada hääle kesksüsteemist allalaadimiseks vajaliku identifikaatori ning häälte krüpteerimiseks kasutatud juhuslikud kontrollkoodid.

Valijarakendus esitab andmestruktuuri `msg-hääle-kontrollkood` QR-koodina [QR] kõrgeimal veaparandustasemel (H). Minimaalselt kodeeritakse andmestruktuuris `msg-hääle-kontrollkood` ühe (1) valimise andmed ehk maksimaalselt 111 baiti informatsiooni. See tingib andmete graafilisel esitamisel vähemalt QR-koodi versiooni 8 kasutamise. Maksimaalselt kodeeritakse andmestruktuuris `msg-hääle-kontrollkood` viie (5) valimise andmed ehk maksimaalselt 391 baiti informatsiooni. See tingib andmete graafilisel esitamisel vähemalt QR-koodi versiooni 17 kasutamise.

Kui samaaegselt on käimas kuus (6) või enam valimist talletatakse kontrollinfo mitmes QR-koodis.

```
msg-hääle-kontrollkood = hääle-identifikaator LF 1*5kontroll-kirje

kontroll-kirje = valimise-identifikaator TAB hex-kontrollkood LF

hääle-identifikaator = 40CHAR

hex-kontrollkood = 40CHAR
; hex-kontrollkood = HEX-ENCODE(kontrollkood)
```

3.5 Kontrollrakenduse sõnum `msg-anna-hääl`

Kontrollitava hääle allalaadimiseks saadab kontrollrakendus kesksüsteemile POST päringu:

- `vote = hääle-identifikaator`

Võimalikud vastussõnumid:

- `msg-kontrollitav-hääl` – Identifikaatoriga hääl oli olemas ning selle kontrollimine oli kesksüsteemi seadetest lähtuvalt võimalik.
- `msg-viga-kontroll` – Kontrollitava hääle alla laadimisel tekkis tehniline või sisuline viga.

3.6 Kesksüsteemi vastussõnum `msg-kontrollitav-hääl`

Selle sõnumiga saab kontrollrakendus kesksüsteemilt kätte krüpteeritud tahteavaldused ning seostatud valikute nimekirja.

```
msg-kontrollitav-hääl = versiooninumber LF olek-ok LF kontroll-konteiner

kontroll-konteiner = valimised LF *krüpteeritud-tahteavaldus LF valikute-nimekiri

krüpteeritud-tahteavaldus = valimise-identifikaator TAB HEX-ENCODE(krüpteeritud-
hääl) LF
```

3.7 Kesksüsteemi vastussõnum `msg-viga-kontroll`

Sõnum on võimalik vastus kõigile kontrollrakenduse päringutele kesksüsteemi. Sõnum tähendab, et kesksüsteem on tuvastanud vea, mis tõkestab hääle kontrollimise.

```
msg-viga-kontroll = versiooninumber LF olek-viga LF vea-kirjeldus
```

4 Kontrolli algoritm

Kontrollrakendus rakendab elektroonilise tahteavalduse protokolli kõigile nimekirja kandidaatidele rakendades QR-koodist saadud juhuarvu. Algoritm on järgmine:

```
procedure kontrolli(hexkood, valikute-nimekiri, krüpteeritud-hääl):
  kood = HEXDECOCE(hexkood)
  foreach valik in valikute-nimekiri:
    tmp = RSAES-OAEP-MOD-ENCRYPT(hlr-avalik-võti, avakujul-hääl(valik)), kood)
    if tmp == krüpteeritud-hääl
      output(valik.valiku-nimi)
  output('ei suutnud tuvastada valikut')

procedure kontrollrakendus(msg-hääle-kontrollkood, msg-kontrollitav-hääl):
  foreach vid = msg-hääle-kontrollkood.valimise-identifikaator:
    if msg-kontrollitav-hääl.contains(vid):
      hexkood =  msg-hääle-kontrollkood[vid].hex-kontrollkood
      valikud =  msg-kontrollitav-hääl[vid].valikute-nimekiri
      krüpteeritud-hääl = msg-kontrollitav-hääl[vid].krüpteeritud-hääl
      kontrolli(hexkood, valikud, krüpteeritud-hääl)
    else:
      output('Hääl ja kontrollinfo ei ole kooskõlalised')
```

5 Sõnum `msg-seadistus`

Sõnum saadetakse vastuseks kontrollrakenduse sõnumile `msg-lae-seadistus`. Seadistused on JSON vormingus, järgneb sõnumi vormingu kirjeldus.

```
msg-seadistus =

{
  "appConfig":{
    "texts":{
      "loading":  Tekst ekraanil aega võtvate tegevuste ajal,
      "welcome_message":  Tervitustekst,
      "lbl_vote":  Hääle kontrollimise kuva pealkiri,
      "lbl_vote_txt":  Hääle kontrollimise kuva tekst,
      "btn_next":  Edasi liikumise nupu tekst,
      "btn_more":  Abiinfo nupu tekst,
      "btn_packet_data":  Nutiseadme andmesidet aktiveeriva nupu tekst,
      "btn_wifi":  Nutiseadme Wifit aktiveeriva nupu tekst,
      "btn_verify":  Kontrolli käivitava nupu tekst,
      "lbl_choice":  Tuvastatud valiku kuva tekst,
      "lbl_close_timeout":  Teavitus rakenduse automaatsest sulgumisest,
      "notification_title":  Teavituse identifikaator,
      "notification_message":  Teavituse sisu,
      "verify_message": Teavitus, et hääl on serveri,
      "close_button": IOS klahvi nimi, mis viib rakenduse lõpust avalehele
   },
   "errors":{
      "no_network_message":  Veateade võrgu puudumisel,
      "problem_qrcode_message":  Veateade QR-koodi lugemisel,
      "close_qrcode_message":  Veateade QR-koodi lugemisel,
      "bad_server_response_message":  Veateade serverilt,
      "bad_verification_message":  Veateade kontrollalgoritmilt
   },
   "colors":{   Kasutajaliidese värvid
      "frame_background":"#AA444444",
      "main_window_foreground":"#FFFFFF",
      "error_window_foreground":"#FFFFFF",
      "loading_window_background":"#33B5E5",
      "loading_window_foreground":"#FFFFFF",
      "main_window":"#33B5E5",
      "main_window_shadow":"#005777",
      "error_window":"#FF0000",
      "error_window_shadow":"#770000",
      "btn_background":"#F0F0F0",
      "btn_foreground":"#727272",
      "btn_verify_foreground":"#FFFFFF",
      "btn_verify_background_start":"#30B4E5",
      "btn_verify_background_center":"#1AABE1",
      "btn_verify_background_end":"#00A1DC",
      "lbl_background":"#33B5E5",
      "lbl_foreground":"#FFFFFF",
      "lbl_shadow":"#008EC2",
      "lbl_outer_container_background":"#EAEAEA",
      "lbl_outer_container_foreground":"#878686",
      "lbl_inner_container_background":"#FFFFFF",
      "lbl_inner_container_foreground":"#878686",
      "lbl_close_timeout_foreground":"#454444",
```

```
      "lbl_close_timeout_background_start":"#FEEC00",
      "lbl_close_timeout_background_center":"#F9D303",
      "lbl_close_timeout_background_end":"#F7C804",
      "lbl_close_timeout_shadow":"#C6A002",
      "lbl_outer_inner_container_divider":"#E9E9E9"
   },
   "params":{
      "app_url":  Kontrollitavaid hääli väljastav URL, enne valimise algust on
välja väärtus tühi
      "help_url":  Rakenduse abiinfo URL,
      "close_timeout":  Rakenduse eluiga peale edukat kontrolli,
      "close_interval":  Taimer,
      "public_key":  HLR avalik võti, BASE64 kodeeringus, ilma reavahetusteta,
enne valimise algust on välja väärtus tühi
   },
   "elections":{
     "VALIMISE ID 1":"Valimise 1 kirjeldus",
     ...
     "VALIMISE ID N":"Valimise N kirjeldus"
   }
  }
}
```

Näide:

Seadistused JSON vormingus – ühe valimise korral enne valimise algust

```
{
   "appConfig":{
          "texts":{
                 "loading":"Oota...",
                 "welcome_message":"Hääle kontrollimiseks peate pildistama arvuti
ekraanil kuvatavat QR-koodi.",
                 "lbl_vote":"Hääle kontrollimine",
                 "lbl_vote_txt":"Teie QR-koodile vastav hääl on talletatud
valimiste serveris.",
                 "btn_next":"Edasi",
                 "btn_more":"Abiinfo",
                 "btn_packet_data":"Andmeside",
                 "btn_wifi":"Wifi",
                 "btn_verify":"Kuva minu valik",
                 "lbl_choice":"Tuvastatud valik",
                 "lbl_close_timeout":"Rakendus sulgub XX sekundi pärast!",
                 "notification_title":"VVK",
                 "notification_message":"Valik on tuvastatud"
                 "verify_message":"Valik serveris",
                 "close_button":"Sulge"
          },
          "errors":{
                 "no_network_message":"Veenduge, et nutiseadme andmeside on
võimaldatud",
                 "problem_qrcode_message":"QR koodi ei õnnestunud tuvastada",
                 "close_qrcode_message":"Lõpetasite QR koodi salvestamise
enneaegselt",
                 "bad_server_response_message":"Tehniline viga, palun teavitage
valimiste läbiviijat",
                 "bad_verification_message":"Viga, ei õnnestunud leida ühtegi
kandidaati kellega krüptogramm kokku sobib"
          },
```

```
          "colors":{
                 "frame_background":"#AA444444",
                 "main_window_foreground":"#FFFFFF",
                 "error_window_foreground":"#FFFFFF",
                 "loading_window_background":"#33B5E5",
                 "loading_window_foreground":"#FFFFFF",
                 "main_window":"#33B5E5",
                 "main_window_shadow":"#005777",
                 "error_window":"#FF0000",
                 "error_window_shadow":"#770000",
                 "btn_background":"#F0F0F0",
                 "btn_foreground":"#727272",
                 "btn_verify_foreground":"#FFFFFF",
                 "btn_verify_background_start":"#30B4E5",
                 "btn_verify_background_center":"#1AABE1",
                 "btn_verify_background_end":"#00A1DC",
                 "lbl_background":"#33B5E5",
                 "lbl_foreground":"#FFFFFF",
                 "lbl_shadow":"#008EC2",
                 "lbl_outer_container_background":"#EAEAEA",
                 "lbl_outer_container_foreground":"#878686",
                 "lbl_inner_container_background":"#FFFFFF",
                 "lbl_inner_container_foreground":"#878686",
                 "lbl_close_timeout_foreground":"#454444",
                 "lbl_close_timeout_background_start":"#FEEC00",
                 "lbl_close_timeout_background_center":"#F9D303",
                 "lbl_close_timeout_background_end":"#F7C804",
                 "lbl_close_timeout_shadow":"#C6A002",
                 "lbl_outer_inner_container_divider":"#E9E9E9"
          },
          "params":{
                 "app_url":"",
                 "help_url":"https://abi.valimised.ee/",
                 "close_timeout":30000,
                 "close_interval":1000,
                 "public_key":""
          },
          "elections":{
                 "TEST2013":"Aasta 2013 testvalimised"

          }
   }
}
```


Seadistused JSON vormingus – ühe valimise korral peale valimise algust


```
{
   "appConfig":{
          "texts":{
                 "loading":"Oota...",
                 "welcome_message":"Hääle kontrollimiseks peate pildistama arvuti
ekraanil kuvatavat QR-koodi.",
                 "lbl_vote":"Hääle kontrollimine",
                 "lbl_vote_txt":"Teie QR-koodile vastav hääl on talletatud
valimiste serveris.",
                 "btn_next":"Edasi",
                 "btn_more":"Abiinfo",
                 "btn_packet_data":"Andmeside",
                 "btn_wifi":"Wifi",
                 "btn_verify":"Kuva minu valik",
                 "lbl_choice":"Tuvastatud valik",
```

```
                "lbl_close_timeout":"Rakendus sulgub XX sekundi pärast!",
                "notification_title":"VVK",
                "notification_message":"Valik on tuvastatud"
                "verify_message":"Valik serveris",
                "close_button":"Sulge"
        },
        "errors":{
                "no_network_message":"Veenduge, et nutiseadme andmeside on
võimaldatud",
                "problem_qrcode_message":"QR koodi ei õnnestunud tuvastada",
                "close_qrcode_message":"Lõpetasite QR koodi salvestamise
enneaegselt",
                "bad_server_response_message":"Tehniline viga, palun teavitage
valimiste läbiviijat",
                "bad_verification_message":"Viga, ei õnnestunud leida ühtegi
kandidaati kellega krüptogramm kokku sobib"
        },
        "colors":{
                "frame_background":"#AA444444",
                "main_window_foreground":"#FFFFFF",
                "error_window_foreground":"#FFFFFF",
                "loading_window_background":"#33B5E5",
                "loading_window_foreground":"#FFFFFF",
                "main_window":"#33B5E5",
                "main_window_shadow":"#005777",
                "error_window":"#FF0000",
                "error_window_shadow":"#770000",
                "btn_background":"#F0F0F0",
                "btn_foreground":"#727272",
                "btn_verify_foreground":"#FFFFFF",
                "btn_verify_background_start":"#30B4E5",
                "btn_verify_background_center":"#1AABE1",
                "btn_verify_background_end":"#00A1DC",
                "lbl_background":"#33B5E5",
                "lbl_foreground":"#FFFFFF",
                "lbl_shadow":"#008EC2",
                "lbl_outer_container_background":"#EAEAEA",
                "lbl_outer_container_foreground":"#878686",
                "lbl_inner_container_background":"#FFFFFF",
                "lbl_inner_container_foreground":"#878686",
                "lbl_close_timeout_foreground":"#454444",
                "lbl_close_timeout_background_start":"#FEEC00",
                "lbl_close_timeout_background_center":"#F9D303",
                "lbl_close_timeout_background_end":"#F7C804",
                "lbl_close_timeout_shadow":"#C6A002",
                "lbl_outer_inner_container_divider":"#E9E9E9"
        },
        "params":{
                "app_url":"https://kontroll.valimised.ee/hes-verify-vote.cgi",
                "help_url":"https://abi.valimised.ee/",
                "close_timeout":30000,
                "close_interval":1000,
                "public_key":"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvaGax2fuVF4B6jysv/Y9/L3WAyHVEdI41ZX7s
ZJYU4TdrgvU3LZgni5D1V4bDyfZBwOGMbx8ixaEp1p3uUsziGAm9rOf7JrO0L2hCw6KH8y580mYvpTZcO
LR4xA6j0SXKyZppi2aqiwbZvbfRD/J8zYW0kZ9/BT9QEBP98IgU/Si7Cn9s6xaDYw3jrlm/8ei8I5fkxm
y2/uWt5dS2MsT3MPFopWnmyVvDLwxFO3epAtf7QM1QBirbOAR+nt5DneVAMtbYxrcMFM06lOwGkOY35Tr
WL3DTJocbtLUNkSZ/fO5V367SCOazuuU82SrU1adyk1SGvrMHrbCwYqIf70OtwIDAQAB-----END
PUBLIC KEY-----"
        },
        "elections":{
                "TEST2013":"Aasta 2013 testvalimised"

        }
   }
```

```
}
```