Avalik

Elektroonilise hääletamise protokollistik II: Hääletamisprotokoll

Dokumendi liik

Redaktsioon: 1.2

18.04.2014

16 lk

Kuupäev	Nr	Kirjeldus	Autor
01.12.2012	0.1	Dokumendi algversioon	Cybernetica AS (Sven Heiberg)
15.01.2013	1.0	Protokolli täpsustused – välja valija defineerimine üldkirjelduses.	Cybernetica AS (Sven Heiberg)
18.07.2013	1.1	Muudatused metaandmetes	Cybernetica AS (Sven Heiberg)
18.04.2013	1.2	Mobiil-ID teenuse uuenemine	Cybernetica AS (Sven Heiberg)

Annotatsioon

Dokument spetsifitseerib valijarakenduse ning kesksüsteemi vahelise elektroonilise hääletamise protokolli.

Sisukord

1 Sissejuhatus

1.1 Hääletamisprotokolli skoop

Hääletamisprotokoll spetsifitseerib valijarakenduse ja elektroonilise hääletamise kesksüsteemi vahelise sõnumivahetuse, mille käigus toimub:

- kesksüsteemi autentimine valijale;
- valija autentimine kesksüsteemile;
- valija ringkonnale vastava valikute/kandidaatide nimekirja saatmine valijarakendusele;
- elektrooniliselt vormistatud tahteavalduse vastuvõtmine valijarakenduselt;
- hääle hilisemaks kontrollimiseks vajaliku informatsiooni saatmine valijarakendusele.

Hääletamisprotokoll sõltub valija autentimiseks ja digitaalallkirja andmiseks kasutatavast elektroonilisest isikutunnistusest. Sõnumivahetus erineb kiipkaardipõhiste tunnistuste (ID-kaart, Digi-ID) ja Mobiil-ID korral. Alljärgnevalt spetsifitseeritakse hääletamisprotokolli mõlemad versioonid.

1.1.1 Üldkirjelduses defineeritud andmestruktuurid

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

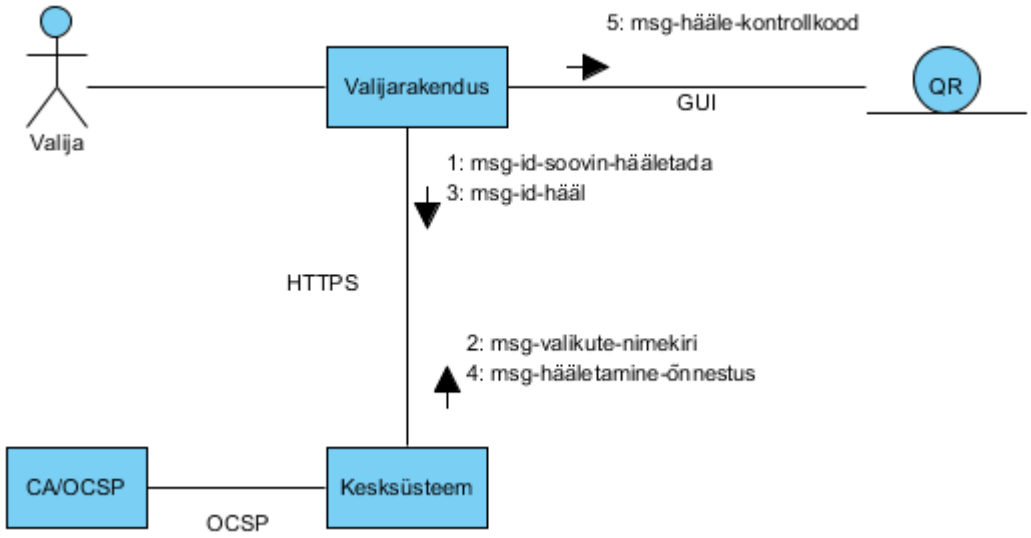
```
hääl-bdoc-idcard

hääl-bdoc-mobid

valikute-nimekiri

valija
```

1.2 Viited

1. [EHI] – Elektroonilise hääletamise protokollistik I: Üldkirjeldus.
2. [HTTPS] – HTTP Over TLS. RFC2818
3. [Mobiil-ID] AS Sertifitseerimiskeskus. DigiDocService spetsifikatsioon. Dokumendi versioon: 2.127. Viimati uuendatud 01.04.2014. Kirjeldatav teenuse versioon: 3.5.*. http://www.sk.ee/files/DigiDocService_spec_est.pdf

2 Sõnumivahetus ID-kaardi/Digi-ID kasutamise korral

Kui valija kasutab kiipkaardipõhist elektroonilist isikutunnistust, siis toimub autentimiseks ja digitaalallkirja andmiseks vajalike signatuuride moodustamine kaardilugeja vahendusel valija arvutiga ühendatud kiipkaardis. Hääletamisprotokoll on sünkroonne.



Joonistus 1: Hääletamisprotokoll, kiipkaart

Hääletamisprotokolli (1) käivitamisele eelneb valijarakenduse käivitamine ning ID-kaardi (Digi-ID) kaardilugejasse asetamine. Protokollis vahetatavad sõnumid, nende järgnevus ja seotud tegevused on järgmised:

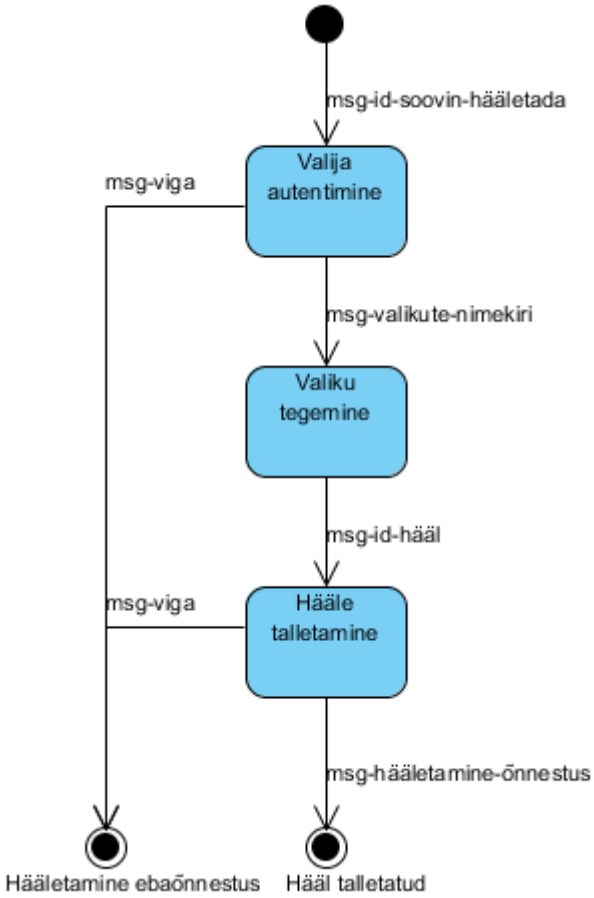
1. Valijarakendus saadab kesksüsteemile sõnumi `msg-id-soovin-hääletada`.
   - SSL võtmevahetuse käigus kontrollivad valijarakendus ja kesksüsteem vastastikku sertifikaate.
   - Valija peab sisestama ID-kaardi PIN1 koodi.
2. Kesksüsteem saadab valijarakendusele sõnumi `msg-valikute-nimekiri`.
   - Sõnum sisaldab autenditud valija ringkonna valikute/kandidaatide nimekirju käimasolevatel valimistel.
   - Valija väljendab valijarakenduse abil valikut tehes oma tahet.
   - Valijarakendus genereerib valija tahteavalduste krüpteerimiseks vajalikud kontrollkoodid, krüpteerib hääled ning allkirjastab krüpteeritud hääled.
   - Valija peab sisestama ID-kaardi PIN2 koodi.
3. Valijarakendus saadab kesksüsteemile sõnumi `msg-id-hääl`.
   - Kesksüsteem pöördub kehtivuskinnituse saamiseks kehtivusteenuse poole.
   - Kui hääle allkirjastamiseks kasutatud sertifikaat on kehtiv, siis tagastab

kehtivusteenus kesksüsteemile kehtivuskinnituse.

- Kesksüsteem talletab hääle, protokolliväliselt spetsifitseeritud aja jooksul on valijal võimalik häält kontrollida.

4. Kesksüsteem saadab valijarakendusele sõnumi `msg-hääletamine-õnnestus`.
   - Sõnum sisaldab unikaalset identifikaatorit, mis on vajalik kontrollprotokollis hääle identifitseerimiseks.
5. Valijarakendus valmendab kontrollrakenduse jaoks sõnumi `msg-hääle-kontrollkood`.
   - Valijarakendus esitab häälte krüpteerimisel kasutatud kontrollkoodid ja hääle unikaalse identifikaatori QR koodina kasutajaliideses.

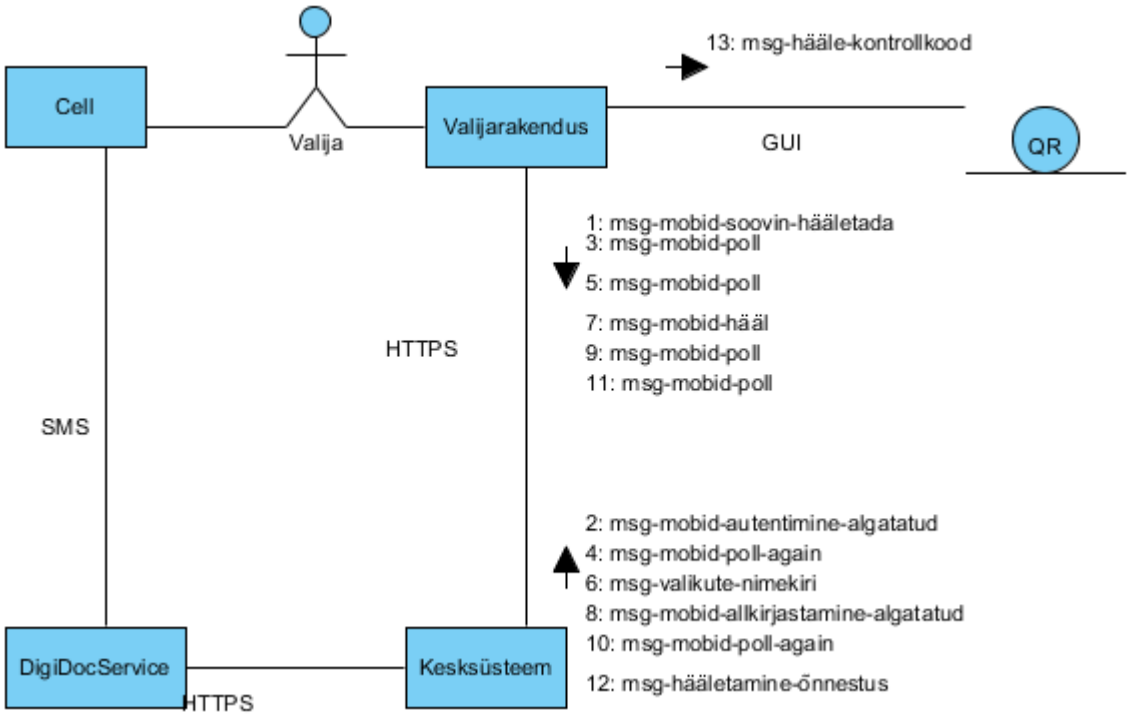
Kui joonistusel 1 on kujutatud üks instants protokollist, siis joonistusel 2 on esitatud hääletamisprotokolli olekumasin ID-kaardi/Digi-ID korral, mis defineerib võimalikud sõnumivahetusstsenaariumid.



Joonistus 2: Hääletamisprotokolli olekumasin, kiipkaart

3 Sõnumivahetus Mobiil-ID kasutamise korral

Kui valija kasutab Mobiil-ID'd, siis toimub autentimiseks ja digitaalallkirja andmiseks vajalike signatuuride moodustamine valija mobiiltelefonis asuvas SIM-kaardis. Autentimis- ja allkirjastamisprotseduurid algatatakse kesksüsteemi poolt Mobiil-ID protokolli [Mobiil-ID] realiseeriva teenuse DigiDocService vahendusel. Hääletamisprotokoll on asünkroonne.



Joonistus 3: Hääletamisprotokoll, Mobiil-ID

Hääletamisprotokolli (3) käivitamisele eelneb valijarakenduse käivitamine. Protokollis vahetatavad sõnumid, nende järgnevus ja seotud tegevused on järgmised:

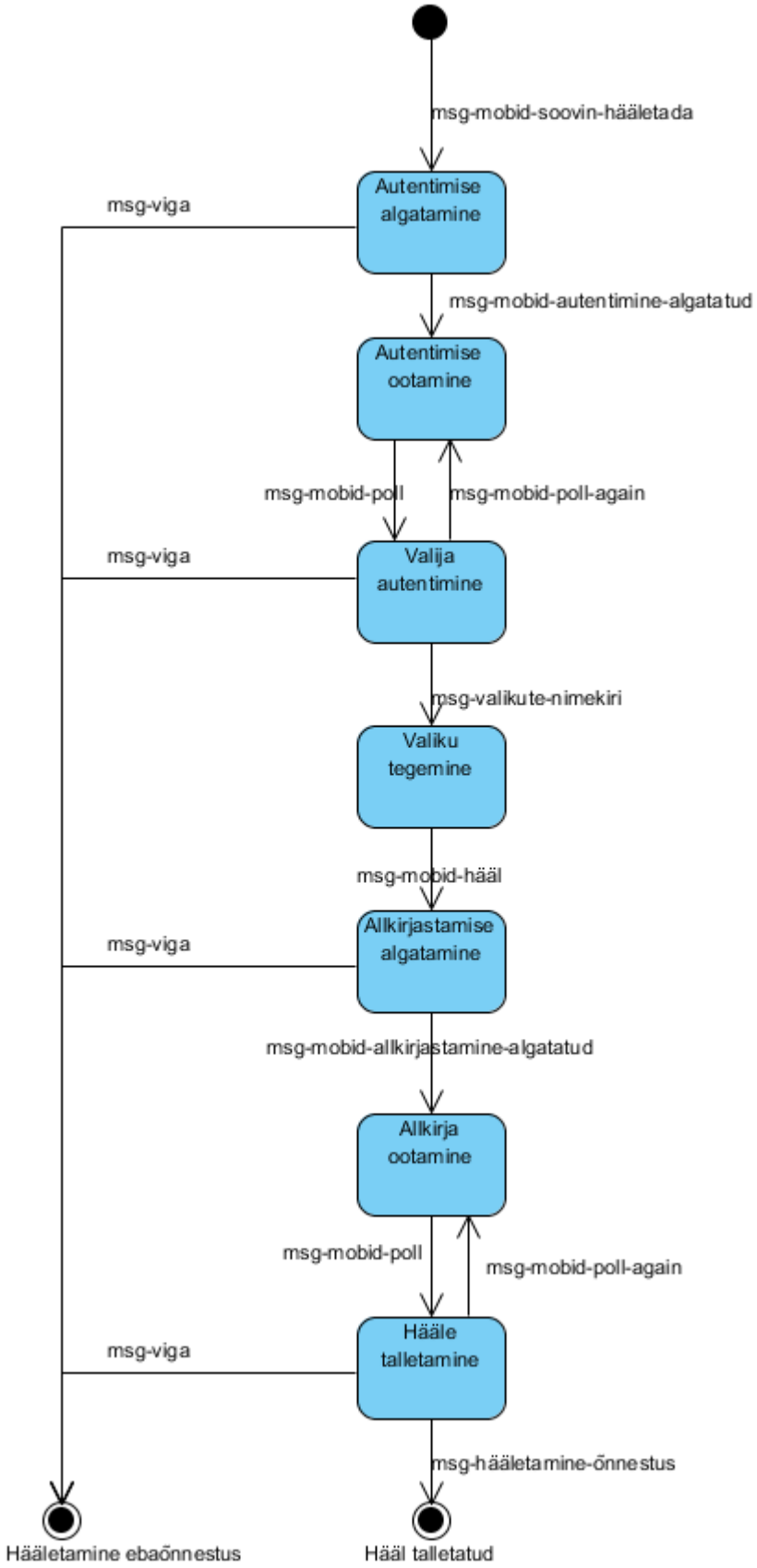
1. Valijarakendus saadab kesksüsteemile sõnumi `msg-mobid-soovin-hääletada`.
   - Sõnum sisaldab valija poolt sisestatud telefoninumbrit.
   - SSL võtmevahetuse käigus kontrollib valijarakendus kesksüsteemi sertifikaati. Kesksüsteemi jaoks on valija enne autentimisprotseduuri lõppu anonüümne.
   - Kesksüsteem algatab Mobiil-ID autentimise pöördudes asünkroonselt teenuse DigiDocService poole päringuga `MobileAuthenticate`.
2. Kesksüsteem saadab valijarakendusele sõnumi `msg-mobid-autentimine-algatatud`.
   - Sõnum sisaldab kesksüsteemi ja DigiDocService'i poolt ühiselt arvutatud Mobiil-ID-koodi.

   - DigiDocService vahendab autentimispäringu etteantud mobiilinumbrile.
3. Valijarakendus saadab kesksüsteemile teatud intervalli tagant sõnumit `msg-mobid-poll`.
4. Kui Mobiil-ID autentimine on veel käimas saadab kesksüsteem valijarakendusele sõnumit `msg-mobid-poll-again`.
   - Valija saab autentimisteate SMS'iga. Valija võrdleb valijarakenduses ning mobiilis kuvatavaid koode ning nende ühtimisel sisestab PIN1'e.
   - Mobiiltelefon vastab DigiDocService autentimispäringule.
   - Iga valijarakenduse pollimise peale pollib kesksüsteem DigiDocService'it.
   - Eduka autentimise korral saab kesksüsteem valija sertifikaadi.
5. Kesksüsteem saadab järgmise pollimise peale valijarakendusele sõnumi `msg-valikute-nimekiri`.
   - Sõnum sisaldab autenditud valija ringkonna valikute/kandidaatide nimekirju käimasolevatel valimistel.
   - Valija väljendab valijarakenduse abil valikut tehes oma tahet.
   - Valijarakendus genereerib valija tahteavalduste krüpteerimiseks vajalikud kontrollkoodid ning krüpteerib hääled.
6. Valijarakendus saadab kesksüsteemile sõnumi `msg-mobid-hääl`.
   - Kesksüsteem algatab Mobiil-ID allkirjastamise pöördudes asünkroonselt teenuse DigiDocService poole päringuga `MobileSign`. Teenusele DigiDocService saadetakse krüpteeritud hääle räsi.
7. Kesksüsteem saadab valijarakendusele sõnumi `msg-mobid-allkirjastamine-algatatud`
   - Sõnum sisaldab kesksüsteemi ja DigiDocService'i poolt ühiselt arvutatud Mobiil-ID-koodi.
   - DigiDocService vahendab allkirjastamispäringu valija poolt sisestatud mobiilinumbrile.
8. Valijarakendus saadab kesksüsteemile teatud intervalli tagant sõnumit `msg-mobid-poll`.
9. Kui Mobiil-ID allkirjastamine on veel käimas saadab kesksüsteem valijarakendusele sõnumit `msg-mobid-poll-again`.
   - Valija saab allkirjastamisteate SMS'iga. Valija võrdleb valijarakenduses ning mobiilis kuvatavaid koode ning nende ühtimisel sisestab PIN2'e.
   - Mobiiltelefon vastab DigiDocService allkirjastamispäringule krüpteeritud hääle räsile antud signatuuriga.
   - Iga valijarakenduse pollimise peale pollib kesksüsteem DigiDocService'it.
   - Eduka allkirjastamise korral saab kesksüsteem kehtivuskinnitusega allkirja.
   - Kesksüsteem talletab hääle, protokolliväliselt spetsifitseeritud aja jooksul on valijal võimalik häält kontrollida.
10. Kesksüsteem saadab järgmise pollimise peale valijarakendusele sõnumi `msg-hääletamine-õnnestus`.

    - Sõnum sisaldab unikaalset identifikaatorit, mis on vajalik kontrollprotokollis hääle identifitseerimiseks.

11. Valijarakendus valmendab kontrollrakenduse jaoks sõnumi `msg-hääle-kontrollkood`.
    - Valijarakendus esitab häälte krüpteerimisel kasutatud kontrollkoodid ja hääle unikaalse identifikaatori QR koodina kasutajaliideses.

Kui joonistusel 3 on kujutatud üks instants protokollist, siis joonistusel 4 on esitatud hääletamisprotokolli olekumasin Mobiil-ID korral, mis defineerib võimalikud sõnumivahetusstsenaariumid.



Joonistus 4: Hääletamisprotkolli olekumasin, Mobiil-ID

4 Protokolli sõnumid

4.1 Sõnumi struktuur

Rakendustaseme hääletamisprotokoll kasutab sõnumivahetuseks HTTPS protokolli [HTTPS]. Valijarakenduse sõnumid esitatakse POST-päringutena etteantud URLile. POST-päringu parameetrite binaarsetele väärtustele rakendatakse BASE64 kodeeringut. 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-viga-sert | olek-viga-valija | olek-
mobid-poll | olek-mobid-viga

olek-ok = 0

olek-viga = 1

olek-viga-sert = 2

olek-viga-valija = 3

olek-mobid-poll = 4

olek-mobid-viga = 5
```

Oleku koode kasutatakse järgmises tähenduses:

- `olek-ok` – operatsioon õnnestus, teate tõlgendamine sõltub protokolli sammust;
- `olek-viga` – viga hääletamisel, täpsem info vea kirjelduses;
- `olek-viga-sert` – valija sertifikaat ei vasta nõuetele, täpsem info vea kirjelduses;
- `olek-viga-valija` – antud isik ei ole kantud ühegi käimasoleva hääletamise valijate nimekirja;
- `olek-mobid-poll` – Mobiil-ID kasutamise korral antakse teada, et vastuse saamiseks tuleb serverit veel pollida, muudes olukordades see kood kasutusel pole;
- `olek-mobid-viga` – Mobiil-ID kasutamisel tekkis viga, muudes olukordades see kood kasutusel pole.

4.2 Valijarakenduse sõnum `msg-id-soovin-hääletada`

ID-kaardi kasutamise korral teeb valijarakendus hääletamisprotokolli algatamiseks kesksüsteemi URLile POST päringu, millel ei ole parameetreid. Päringu tulemusena

luuakse vastastikuselt autenditud SSL-ühendus.

Võimalikud vastussõnumid:

- `msg-valikute-nimekiri` – autentimine õnnestus, sertifikaadist tuvastatud isikukood oli mõnel käimasoleval valimisel valijate nimekirjas, valijarakendusele tagastatakse vastavate ringkondade valikute nimekirjad.
- `msg-viga` – valikute nimekirja väljastamine ei õnnestunud kas tehnilistel või sisulistel põhjustel.

4.3 Valijarakenduse sõnum `msg-mobid-soovin-hääletada`

Mobiil-ID kasutamise korral teeb valijarakendus hääletamisprotokolli algatamiseks kesksüsteemi URLile POST päringu:

- `phone = mobid-telefoninumber`.

Väli `mobid-telefoninumber` sisaldab hääletaja telefoninumbrit.

```
mobid-telefoninumber = „+".telefoninumber

telefoninumber = 10*15DIGIT
```

Võimalikud vastussõnumid:

- `msg-mobid-autentimine-algatatud` – Mobiil-ID autentimine on algatatud, valijarakendus peab mõne aja möödudes kesksüsteemi pollima.
- `msg-viga` – autentimise algatamine ei õnnestunud kas tehnilistel või sisulistel põhjustel.

4.4 Kesksüsteemi vastussõnum `msg-mobid-autentimine-algatatud`

Sõnum saadetakse vastuseks valijarakenduse sõnumile `msg-mobid-soovin-hääletada`. Sõnum sisaldab:

- DigiDocService'i poolt genereeritud koodi, mida kuvatakse nii valijarakenduses kui mobiiltelefonis,
- seansiidentifikaatorit, mida valimisrakendus peab kasutama järgneva sõnumivahetuse vältel.

```
msg-mobid-autentimine-algatatud = versiooninumber LF olek-ok LF
seansiidentifikaator TAB mobid-kood

seansiidentifikaator = 1*24ASCIICHAR

mobid-kood = 4DIGIT
```

4.5 Kesksüsteemi vastussõnum `msg-mobid-allkirjastamine-algatatud`

Sõnum saadetakse vastuseks valijarakenduse sõnumile `msg-mobid-hääl`. Sõnum sisaldab DigiDocService'i poolt genereeritud koodi, mida kuvatakse nii valijarakenduses kui mobiiltelefonis.

```
msg-mobid-allkirjastamine-algatatud = versiooninumber LF olek-ok LF mobid-kood
```

4.6 Valijarakenduse sõnum `msg-mobid-poll`

Mobiil-ID kasutamise korral toimuvad autentimine ja allkirjastamine asünkroonselt ning valijarakendus peab kesksüsteemi tulemusest teada saamiseks pollima. Selleks saadab valijarakendus HES'ile POST päringu:

- `session = seansiidentifikaator`
- `poll = true`

```
true = „true“
```

Võimalikud vastussõnumid:

- `msg-mobid-poll-again` – Käimasoleva operatsiooni tulemus ei ole veel selgunud, valijarakendus peab mõne aja möödudes uuesti proovima.
- `msg-valikute-nimekiri` – autentimine õnnestus, sertifikaadist tuvastatud isikukood oli mõnel käimasoleval valimisel valijate nimekirjas, valijarakendusele tagastatakse vastavate ringkondade valikute nimekirjad.
- `msg-hääletamine-õnnestus` – hääle talletamine õnnestus.
- `msg-viga` – autentimise algatamine ei õnnestunud kas tehnilistel või sisulistel põhjustel.

4.7 Kesksüsteemi vastussõnum `msg-mobid-poll-again`

Sõnum saadetakse vastuseks valijarakenduse sõnumile `msg-mobid-poll`. Käimasolev Mobiil-ID autentimine või allkirjastamine ei ole veel tulemuseni jõudnud.

```
msg-mobid-poll-again = versiooninumber LF olek-mobid-poll LF
```

4.8 Kesksüsteemi vastussõnum `msg-valikute-nimekiri`

Sõnum saadetakse vastuseks valijarakenduse sõnumile `msg-id-soovin-hääletada` või sõnumile `msg-mobid-poll`. Sõnum tähendab, et autentimine õnnestus ja sertifikaadist

tuvastatud isikukood oli mõnel käimasoleval valimisel valijate nimekirjas. Sõnum sisaldab vastavate ringkondade valikute nimekirju.

Väljaga `valimised` edastatakse valijarakendusele info selle kohta, mis tüüpi valimised nimekirjas on. Iga valikute nimekirjas esineva valimiste identifikaatori kohta peab olema ära toodud valimiste tüüp.

Väli `seansiidentifikaator` sisaldab endas unikaalset identifikaatorit, mis hiljem lisatakse hääle talletamise päringule POST parameetriks.

Väli `valija` annab valijarakendusele infot autenditud isiku kohta. Väli on vajalik, kuna Mobiil-ID'ga autentides ei tea valijarakendus valija identiteeti.

Koos valikute nimekirjaga informeerib server valijat ka sellest, kas viimane on eelnevalt hääletanud või mitte. Juhul kui kasutaja valik on serveris juba talletatud lisatakse valikute nimekirja lõppu serveripoolne teade, mis sisaldab infot talletatud hääle kohta. Kui kasutaja ei ole hääletanud, siis teadet ei lisata.

```
msg-valikute-nimekiri = versiooninumber LF olek-ok LF nimekiri

nimekiri = nimekiri-algne | nimekiri-korduv

nimekiri-algne = *valimised LF seansiidentifikaator LF valija LF valikute-
nimekiri

nimekiri-korduv = *valimised LF seansiidentifikaator LF valija LF valikute-
nimekiri LF korduv

valimised = valimise-identifikaator ':' valimise-tyyp TAB

korduv = "korduv" TAB selgitus

selgitus = 1*100UTF-8-CHAR
```

4.9 Valijarakenduse sõnum `msg-id-hääl`

ID-kaardiga allkirjastatud hääle kesksüsteemile saatmiseks saadab valijarakendus POST päringu:

- `session = seansiidentifikaator`
- `vote = BASE64(hääl-bdoc-idcard)`

Võimalikud vastussõnumid:

- `msg-hääletamine-õnnestus` – hääle talletamine õnnestus.
- `msg-viga` – hääle talletamine ei õnnestunud kas tehnilistel või sisulistel põhjustel.

4.10 Valijarakenduse sõnum `msg-mobid-hääl`

Hääle allkirjastamiseks Mobiil-ID'ga saadab valijarakendus kesksüsteemile POST päringu:

- `session = seansiidentifikaator`
- `vote = BASE64(hääl-bdoc-mobid)`

Võimalikud vastussõnumid:

- `msg-mobid-allkirjastamine-algatatud` – Mobiil-ID allkirjastamine on

algatatud, valijarakendus peab mõne aja möödudes kesksüsteemi pollima.

- `msg-viga` – allkirjastamise algatamine ei õnnestunud kas tehnilistel või sisulistel põhjustel.

4.11 Kesksüsteemi vastussõnum `msg-hääletamine-õnnestus`

Sõnum saadetakse vastuseks valijarakenduse sõnumile `msg-id-hääl` või sõnumile `msg-mobid-poll`. Sõnum tähendab, et allkirjastatud hääl on kesksüsteemis edukalt talletatud. Sõnum sisaldab talletatud häälele viitavat unikaalset identifikaatorit.

```
msg-hääletamine-õnnestus = versiooninumber LF olek-ok LF hääle-identifikaator

hääle-identifikaator = 40CHAR
```

4.12 Kesksüsteemi vastussõnum `msg-viga`

Sõnum on võimalik vastus kõigile valijarakenduse päringutele. Sõnum tähendab, et kesksüsteem on tuvastanud vea, mis tõkestab antud hääletamise.

```
msg-viga = versiooninumber LF vea-kood LF vea-kirjeldus

vea-kood = olek-viga | olek-viga-sert | olek-viga-valija | olek-mobiil-id-keeld |
olek-mobiil-id-viga

vea-kirjeldus = 1*100UTF-8-CHAR
```