Avalik

Elektroonilise hääletamise protokollistik I: Üldkirjeldus

Dokumendi liik

Redaktsioon: 1.1

18.04.2014

14 lk

Kuupäev	Nr	Kirjeldus	Autor
01.12.2012	0.1	Dokumendi algversioon	Cybernetica AS (Sven Heiberg)
15.01.2013	1.0	Kontrollprotokolli täpsustus: digitaalse templi eemaldamine. Välja valija defineerimine üldkirjelduses.	Cybernetica AS (Sven Heiberg)
18.04.2014	1.1	BDOC2.1 vorming, suletud nimekirjade eemaldamine	Cybernetica AS (Sven Heiberg)

Annotatsioon

Dokument annab üldise ülevaate elektroonilise hääletamise süsteemi tehnilisest ülesehitusest ja kasutatavatest protokollidest. Dokumendis defineeritakse protokollides kasutatavad ühised mõisted ja andmestruktuurid.

Sisukord

1 Sissejuhatus.....5
1.1 Töö eesmärk.....5
1.2 Viited.....5
2 Elektroonilise hääletamise protokollistik.....7
2.1 Elektroonilise hääletamise protokollistiku versioon.....7
2.2 Valija isikuandmed.....7
2.3 Samaaegsed valimised.....7
2.4 Valimisringkonnad erituubilistel valimistel.....8
2.5 Valija tahteavaldus.....10
3 Elektroonilise tahteavalduse protokoll.....11
3.1 Protokolli kontseptsioon.....11
3.2 Elektroonilise hääle formaat.....12
3.3 Krüpteeritud elektrooniline hääl.....12
3.4 Digitaalselt allkirjastatud hääl.....13

1 Sissejuhatus

1.1 Töö eesmärk

Elektroonilise hääletamise protokollistik (edaspidi protokollistik) defineerib elektroonilise hääletamise süsteemi komponentide vahelise sõnumivahetuse, kasutatavad andmestruktuurid, algoritmid ning liidesed väliste süsteemidega.

Sõnumivahetus esitatakse UML suhtlusskeemidena, mis üheselt defineerivad sõnumite järgnevuse. Andmestruktuuride kirjeldused on varustatud Backus-Naur notatsioonis spetsifikatsioonidega. Andmestruktuuride väljade eraldajateks kasutatakse reavahetuse sümbolit `LF`, ASCII-koodiga `0x0A` ja tabulaatori sümbolit `TAB`, ASCII-koodiga `0x09`. Algoritmid esitatakse pseudokoodina.

Protokollistiku kirjeldus jaguneb nelja dokumendi vahele:

- Üldkirjeldus [EHI] – protokollistiku erinevate osade ühised andmestruktuurid, elektroonilise tahteavalduse protokoll.
- Hääletamisprotokoll [EHII] – valijarakenduse ja kesksüsteemi vaheline hääletamisprotokoll.
- Kontrollprotokoll [EHIII] – valijarakenduse, kesksüsteemi ja kontrollrakenduse vaheline kontrollprotokoll.
- Kesksüsteemi protokollid [EHIV] – andmestruktuurid kesksüsteemi liidestamiseks valimiste infosüsteemi ja rahvastikuregistriga, protokollid kesksüsteemi komponentide HES, HTS ja HLR vahel, protokollid kesksüsteemi komponentide ja Mobiil-ID teenuse ning kehtivuskinnitusteenuse vahel.

1.2 Viited

1. [EHAK] - Eesti haldus- ja asustusjaotuse klassifikaator 2012v2, Eesti Statistikaamet, http://metaweb.stat.ee/
2. [EHI] – Elektroonilise hääletamise protokollistik I: Üldkirjeldus.
3. [EHII] – Elektroonilise hääletamise protokollistik II: Hääletamisprotokoll.
4. [EHIII] – Elektroonilise hääletamise protokollistik III: Kontrollprotokoll.
5. [EHIV] – Elektroonilise hääletamise protokollistik IV: Kesksüsteemi protokollid.
6. [EPVS] – Euroopa Parlamendi valimise seadus (RT I 2003, 4, 22)
7. [BDOC2.1] – BDOC. Digitaalallkirja vorming. Versioon 2.1:2013. http://www.id.ee/public/bdoc-spec21-est.pdf
8. [KOVVS] – Kohaliku omavalitsuse volikogu valimise seadus (RT I 2002, 36, 220)
9. [OCSP] – Online Certificate Status Protocol (RFC2560)
10. [RHS] – Rahvahääletuse seadus (RT I 2002, 30, 176)
11. [RKVS] – Riigikogu valimise seadus (RT I 2002, 57, 355)
12. [RSA-OAEP] – PKCS #1: RSA Cryptography Standard, RSA Security, 21.06.2005,

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

13. [X509] – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)

2 Elektroonilise hääletamise protokollistik

2.1 Elektroonilise hääletamise protokollistiku versioon

Protokollistik arvestab ajalise muutumise võimalusega, mis võib rikkuda tagasiühilduvuse. Andmestruktuurid sisaldavad välja `versiooninumber`, mille pikkus on piiratud 2 tähemärgiga. Välja väärtus on positiivne täisarv. Käesolevale spetsifikatsioonile vastavate andmestruktuuride puhul on versiooninumbriks `1`. Spetsifikatsiooni realiseerivad rakendused peavad keelduma töötlemast muude versiooninumbritega andmeid.

```
versiooninumber = 1*2DIGIT
```

NB! Kõigis protokollistiku andmestruktuuride väljades tuleb rangelt kinni pidada lubatud sümbolitest ning väljade minimaalsetest-maksimaalsetest pikkustest. Täiendavate tühikute, tabulaatorite jms. kasutamine on keelatud ning spetsifikatsiooni realiseerivad rakendused peavad formaadile mitte-vastavate andmete töötlemisest keelduma.

2.2 Valija isikuandmed

Osades protokollistiku protokollides on vajadus teavitada komponente valija isikust. Nii Mobiil-ID'ga hääletamise kui hääle kontrollimise korral teab kesksüsteem valija isikut, kuid infot vajavatele komponentidele – valijarakendusele või kontrollrakendusele tuleb see eraldi esitada. Sellisel juhul kasutatakse alljärgnevat andmestruktuuri.

```
valija = valija-nimi TAB valija-isikukood

valija-nimi = 1*100UTF-8-CHAR

valija-isikukood = 11DIGIT
```

2.3 Samaaegsed valimised

Elektroonilise hääletamise protokollistik toetab mitme eritüübilise valimise läbiviimist samaaegselt. Andmestruktuurides erinevate valimiste kohta käiva informatsiooni eristamiseks kasutatakse välja `valimise-identifikaator`. Välja pikkus on piiratud 28 tähemärgiga ASCII kooditabelist. Konkreetse valimise tarbeks kasutatav identifikaator spetsifitseeritakse igakordselt kesksüsteemi seadistustes. Spetsifikatsiooni realiseerivad rakendused peavad keelduma töötlemast andmeid, mis identifitseerivad valimise, mis ei kuulu rakenduse jaoks seadistatud valimiste nimekirja. Väljaga `valimise-identifikaator` märgendatud kirjeid tohib kasutada ainult identifitseeritud valimise kontekstis.

```
valimise-identifikaator = 1*28CHAR
```

2.4 Valimisringkonnad eritüübilistel valimistel

Protokollistik toetab eritüübiliste valimiste läbiviimist. Eristatakse Kohalike Omavalitsuste Volikogude (KOV) valimisi, Riigikogu valimisi, Euroopa Parlamendi valimisi ning rahvahääletusi. Erinevatel valimistel võivad andmestruktuurid ning toimingud nendega erineda, seetõttu tuleb protokollides erinevate valimiste tüüpide vahel vahet teha.

```
valimise-tyyp = tyyp-kov | tyyp-rh | tyyp-rk | tyyp-euro

tyyp-rh = 0

tyyp-kov = 1

tyyp-rk = 2

tyyp-euro = 3
```

Tüüpide ja reaalsete valimiste vaheline vastavus on järgmine:

- `tyyp-rh` – rahvahääletus vastavalt seadusele „Rahvahääletuse seadus“ [RHS]
- `tyyp-kov` – KOV valimised vastavalt seadusele „Kohaliku omavalitsuse volikogu valimise seadus“ [KOVVS]
- `tyyp-rk` – Riigikogu valimised vastavalt seadusele „Riigikogu valimise seadus“ [RKVS]
- `tyyp-euro` – Europarlamendi valimised vastavalt seadusele „Euroopa Parlamendi valimise seadus“ [EPVS]

Erinevad valimised toimuvad erinevatel tasanditel:

- `tyyp-rh, tyyp-rk, tyyp-euro` – valimine toimub riigi tasandil, hääletamistulemus on kõigile kohalikele omavalitsustele ühine;
- `tyyp-kov` – valimine toimub kohaliku omavalitsuse tasandil, igal omavalitsusel on oma hääletamistulemus.

Valimiste järgmise tasandi liigendus on jagunemine valimisringkondadeks:

- `tyyp-rh` – terve riik on üks suur valimisringkond;
- `tyyp-kov` – valimisringkonnad moodustatakse omavalitsuse tasemel vastavalt seaduses kirjeldatud reeglitele;
- `tyyp-rk` – riigis on 12 valimisringkonda;
- `tyyp-euro` – terve riik on üks suur valimisringkond;

Kandidaate on võimalik valimisele üles seada ainult konkreetses valimisringkonnas.

Ringkonnad jagunevad jaoskondadeks ning valijad jaotatakse jaoskondade vahel. Kõigis ühe ringkonna jaoskondades saavad konkreetse jaoskonna alla kuuluvad valijad hääletada selle ringkonna kandidaatide poolt. Valija jaoskonnakuuluvuse kaudu on määratud ka tema ringkonnakuuluvus. Valija saab teha valiku ainult tema ringkonnas kandideerivate valikute vahel.

Kuna kohaliku omavalitsuse volikogude valimisel toimub valimine Eesti omavalitsuste – vallad, linnad – tasemel, siis kasutatakse elektroonilise hääletamise protokollistikus valimisringkondade, -jaoskondade kirjeldamisel ning valijate ja valikute ringkonnakuuluvuse näitamisel Eesti haldus- ja asustusjaotuse klassifikaatorit [EHAK]:

- Tallinna linna EHAK kood on 784.
- Aegviidu valla EHAK kood on 112.

Riigi tasemel toimuvatel valimistel (`tyyp-rh, tyyp-rk, tyyp-euro`) pannakse ringkonna EHAK koodiks kokkuleppeliselt 0. Valimisjaoskondade EHAK koodiks pannakse selle omavalitsuse kood, mille koosseisus konkreetne jaoskond on moodustatud.

```
ehak-kood = 1*10DIGIT

ringkonna-ehak-kood = ehak-kood

ringkond = ringkonna-ehak-kood TAB ringkonna-number-omavalitsuses

ringkonna-number-omavalitsuses = 1*10DIGIT


jaoskonna-ehak-kood = ehak-kood

jaoskond = jaoskonna-ehak-kood TAB jaoskonna-number-omavalitsuses TAB ringkond

jaoskonna-number-omavalitsuses = 1*10 DIGIT


ringkonna-nimi = 1*100UTF-8-CHAR

jaoskonna-nimi = 1*100UTF-8-CHAR

maakonna-nimi = 1*100UTF-8-CHAR
```

Väli `jaoskonna-nimi` sisaldab jaoskonna omavalitsuse EHAK-täisnime. Võimalik on üks kolmest kujust:

- `riik, maakond, vald, jaoskond`: Eesti Vabariik, Harju maakond, Anija vald, valimisjaoskond nr. 1
- `riik, maakond, linn, jaoskond`: Eesti Vabariik, Harju maakond, Maardu linn, valimisjaoskond nr. 1
- `riik, maakond, linn, linnaosa, jaoskond`: Eesti Vabariik, Harju maakond, Tallinn, Kristiine linnaosa, valimisjaoskond nr. 1

Erandina on välismaal hääletanute jaoks loodud jaoskondade nimi kujul:

- `ringkond, jaoskond`: Ringkond 1, valimisjaoskond nr. 1

Riigikogu ja europarlamendi valimistel ning rahvahääletusel moodustatakse valimisjaoskondade ja –ringkondade nimekirjas igasse ringkonda fiktiivne jaoskond välismaal hääletajate tarbeks. Välismaalaste puhul valimisjaoskonna number KOV koodiga näeb välja `0 TAB 0`.

2.5 Valija tahteavaldus

Valijale elektroonilise hääletamise käigus nähtavaid valimiste vahelisi süsteemseid erinevusi on kolm:

- Rahvahääletusel ei valita erakondadesse kuuluvate kandidaatide vahel vaid vastatakse „JAH“/“EI“ konkreetsetele küsimustele.
- Riigikogu, KOV ja Euroopa Parlamendi valimistel antakse hääl ühele kandidaadile, kes võib, aga ei pruugi kuuluda suuremasse erakonda/nimekirja.

Kõigil valimise tüüpidel on valija valik kodeeritav ühe arvväärtusena:

- rahvahääletusel vastusevariandi number,
- valimisel kandidaadi number,

Protokollistik kodeerib valija valiku kuni 11-kohalise arvväärtusena. Tahteavalduse kodeerimiseks lisatakse valija valikule ringkonna omavalitsuse number, mis KOV valimiste korral identifitseerib omavalituse, kus kandidaat kandideerib. Valijale tohivad kättesaadavad olla ainult tema ringkonnakohased valikud. Valijarakendus peab seda omadust tagama ning häältelugemisrakendus kontrollima.

```
valiku-kood = 1*11DIGIT

tahteavaldus = ringkonna-ehak-kood'.'valiku-kood
```

Võimalikud tahteavaldused esitatakse valijarakendusele valikute nimekirjana.

```
valikute-nimekiri = *valiku-rida

valiku-rida = valimise-identifikaator TAB valiku-kirje

valiku-id = tahteavaldus

valiku-kirje = *1ringkonna-number-omavalitsuses TAB *1ringkonna-nimi TAB valiku-
id TAB valiku-nimi TAB *1valimisnimekirja-nimi LF

valiku-nimi = 1*100UTF-8-CHAR

kandidaadi-nimi = 1*100UTF-8-CHAR

valimisnimekirja-nimi = 1*100UTF-8-CHAR
```

Valiku nimi on valimise puhul kandidaadi nimi ning rahvahääletusel vastusevariant. Valimisnimekirja nimi viitab erakonnale või nimekirjale kuhu kandidaat kuulub. Rahvahääletusel ning üksikkandidaatide puhul jäetakse see väli tühjaks.

Juhul, kui samaaegselt esitatakse mitu küsimust, sisaldab valikute nimekiri mitme erineva valimiste identifikaatoriga valikuid. Sama identifikaatoriga valikud kuvatakse koos. Mitme küsimuse korral esitab rakendus järjest mitu valikut.

3 Elektroonilise tahteavalduse protokoll

3.1 Protokolli kontseptsioon

Elektroonilise tahteavalduse protokoll spetsifitseerib valija tahteavalduse elektroonilise vormistamise valija arvutis ning andmeformaadid tahteavalduse talletamiseks ja töötlemiseks kesksüsteemis. Elektroonilise tahteavalduse protokoll spetsifitseerib

- elektroonilise hääle formaadi, mis võimaldab üheselt määratleda valija tahte konkreetsel valimisel;
- elektroonilise hääle krüpteerimise hääletamise salajasuse tagamiseks;
- elektroonilise hääle digitaalse allkirjastamise tervikluse ja valija identifitseerimise tagamiseks;
- elektroonilise hääle digitaalse tembeldamise kesksüsteemi poolt, hääle vastu võtmise tähistamiseks;

Protokoll eeldab, et kesksüsteemis on genereeritud PKCS#1 standardikohane RSA võtmepaar [RSA-OAEP] (`hlr-avalik-võti`, `hlr-privaatvõti`) ning paari avalik komponent on tehtud valijarakendusele kättesaadavaks andmestruktuuri `hlr-sertifikaat` kujul. Protokolli vahendusel liigub valija tahe kesksüsteemi ning võetakse tulemuse kujunemisel arvesse järgmist sündmusterida pidi:

- Valija kasutab valijarakendust oma tahteavalduse vormistamiseks elektrooniliselt:
  - iga käimasoleva valimise kohta, kus valija on volitatud osalema:
    - vormistatakse tahteavaldus elektroonilise häälena (`avakujul-hääl`),
    - vormistatud hääl krüpteeritakse (`hlr-sertifikaat`, `hlr-avalik-võti`, `kontrollkood`, `krüpteeritud-hääl`),
  - kõigi käimasolevate valimiste krüpteeritud hääled allkirjastatakse ühiselt digitaalselt (`hääl-bdoc-idcard`, `hääl-bdoc-mobid`).
- Kesksüsteem talletab elektroonilise hääle:
  - digitaalselt allkirjastatud häälele võetakse valija sertifikaadi kehtivuskinnitus (`hääl-bdoc`),
- Kesksüsteem arvutab hääletamistulemuse:
  - krüpteeritud hääled ja digitaalallkirjad eraldatakse (`krüpteeritud-hääl`),
  - erinevate valimiste kontekstis antud hääled grupeeritakse valimise identifikaatori alusel,
  - iga valimise krüpteeritud hääled dekrüpteeritakse teistest valimistest sõltumatult (`hlr-privaatvõti`, `krüpteeritud-hääl`),
  - dekrüpteeritud häälte põhjal (`avakujul-hääl`) arvutatakse hääletamistulemus.

Protokoll on analoogne paberil posti teel hääletamise protokolliga, kus valija tahe liigub valimiskomisjonini kahes ümbrikus – välimise ümbriku sees on sisemine ümbrik, mis omakorda sisaldab valija tahteavaldusega hääletussedelit. Välimine ümbrik kannab valijat

identifitseerivat informatsiooni ning võimaldab mh. kontrollida valija õigust hääletada. Sisemine ümbrik on anonüümne ning kaitseb hääle salajasust. Enne häälte kokkulugemist eraldatakse sisemised ümbrikud välimistest.

Elektroonilise hääletamise kontekstis on sisemine ümbrik vormistatud krüpteeritud häälena ning välimine ümbrik digitaalselt allkirjastatud dokumendina.

3.2 Elektroonilise hääle formaat

Avakujul hääl koosneb kolmest andmeväljast – `versiooninumber`, `valimise-identifikaator` ja `tahteavaldus`.

```
avakujul-hääl = versiooninumber LF valimise-identifikaator LF tahteavaldus LF
```

Formaadile vastava avakujul hääle maksimaalne võimalik pikkus on 53 baiti.

3.3 Krüpteeritud elektrooniline hääl

Krüpteeritud elektrooniline hääl saadakse avakujul häälele PKCS#1 standardis [RSA-OAEP] defineeritud RSAES-OAEP krüpteerimisalgoritmi (identifikaator: `rSAES-OAEP-Default-Identifier`) modifikatsiooni `RSAES-OAEP-MOD-ENCRYPT` rakendades. Kui standardne RSAES-OAEP defineerib OAEP polsterfunktsiooni jaoks vajaliku juhuarvu `seed` (edaspidi `kontrollkood`) genereerimise krüpteerimisalgoritmi `RSAES-OAEP-ENCRYPT` sammuna 2.d [RSA-OAEP], siis elektroonilise tahteavalduse protokollis genereeritakse `kontrollkood` enne krüpteerimismeetodi käivitamist ning antakse meetodile sisendina. Antud muudatus on vajalik kontrollprotokolli realiseerimiseks ning see ei vähenda turvalisust võrreldes krüpteerimisalgoritmi poolse genereerimisega, kui täidetud on järgmised tingimused:

- juhuarvu genereerimine toimub krüpteerivas seadmes, vahetult enne krüpteerimist;
- juhuarvu genereerimiseks kasutatakse krüpteerimisalgoritmi poolt kasutatavat meetodit.

Krüpteerimiseks kasutatakse avalikku võtit (`hlr-avalik-võti`), millele vastav privaatvõti (`hlr-privaatvõti`) on kasutusel häältelugemisrakenduses. Avalik võti esitatakse PKCS#1 standardis defineeritud ASN.1 andmestruktuurina `RSAPublicKey`. Privaatvõti esitatakse PKCS#1 standardis defineeritud ASN.1 andmestruktuurina `RSAPrivateKey`. Valijarakenduse jaoks tehakse avalik võti kättesaadavaks standardis X.509 defineeritud ASN.1 andmestruktuurina `Certificate` esitatud sertifikaadi koosseisus [X509]. Sertifikaadi DER-kodeeringut võib levitada PEM-kodeeritud kujul. Sertifikaat allkirjastatakse häältelugemisrakenduse privaatvõtmega.

Krüpteeritud elektroonilise hääle avakujule teisendamiseks kasutatakse standardset algoritmi `RSA-OAEP-DECRYPT`.

RSAES-OAEP algoritmi rakendamisele kehtivad järgmised kitsendavad tingimused:

- RSAES-OAEP algoritmi poolt võimaldatavaks märgendiks on tühi string;
- Kasutatava RSA võtmepaari mooduli `n` pikkus on 2048 bitti;
- RSA avaliku eksponendi väärtus on `65537`;

- OAEP räsifunktsioonidena kasutatakse funktsiooni SHA-1;
- OAEP maskigeneraatorina kasutatakse funktsiooni MGF1;

Neist tingimustest tulenevalt on

- genereeritava kontrollkoodi pikkus 160 bitti (20 baiti),
- krüpteeritava avakujul hääle maksimaalne võimalik pikkus 1712 bitti (214 baiti),
- krüpteeritud hääle pikkus 2048 bitti (256 baiti).

```
hlr-avalik-võti = RSAPublicKey (ASN.1, PKCS#1)

hlr-privaatvõti = RSAPrivateKey (ASN.1, PKCS#1)

hlr-sertifikaat = Certificate (ASN.1, X509)

kontrollkood = 160BIT

krüpteeritud-hääl = 2048BIT

; Andmestruktuuride krüpteeritud-hääl ja avakujul-hääl vaheline seos:
;
; krüpteeritud-hääl =
;         RSAES-OAEP-MOD-ENCRYPT(hlr-avalik-võti, avakujul-hääl, juhuarv)
; avakujul-hääl =
;         RSAES-OAEP-DECRYPT(hlr-privaatvõti, krüpteeritud-hääl)
```

3.4 Digitaalselt allkirjastatud hääl

Krüpteeritud hääl tuleb enne kesksüsteemi saatmist digitaalselt allkirjastada, milleks on võimalik kasutada kõiki Eesti Vabariigis kehtivaid digitaalallkirjavahendeid – ID-kaart, Digi-ID, Mobiil-ID. Spetsifikatsioon näeb ette Eesti Vabariigi Standardikavandis [BDOC2.1] defineeritud BDOC allkirjavormingu kasutamise. BDOC allkirjavorming koosneb ETSI standardi TS 101 903 (XadES) profiilist ning OpenDocument konteineri vormingust.

Olenevalt käimasolevate valimiste arvust võib digitaalselt allkirjastatud hääl sisaldada ühte või mitut andmefaili MIME tüübiga `application/x-encrypted-vote`. Iga andmefaili sisuks on `krüpteeritud-hääl`. Andmefaili ja teiste signeeritavate andmeobjektide räsimiseks enne allkirjastamist kasutatakse räsifunktsiooni SHA-256. Andmefaili nimi moodustatakse laiendist 'evote' ning selle valimise identifikaatorist, kus antud hääl arvesse peab minema. Kõik viidatud andmefailid peavad allkirjakonteineris sisalduma. Digitaalselt allkirjastatud hääl ei tohi sisaldada muid andmefaile kui neid, mis sisaldavad hääli mõne käimasoleva valimise kontekstis. Seadistusele mittevastavate häälte vastuvõtmisest, talletamisest ja töötlemisest peab kesksüsteem keelduma.

```
andmefaili-nimi = valimise-identifikaator.laiend

laiend = „evote“
```

Valijarakenduses ID-kaardi või Digi-ID'ga allkirjastatud hääl (`hääl-bdoc-idcard`) peab olema BDOC-BES vormingus. Digitaalselt allkirjastatud häälele BDOC-BES vormingus on seatud järgmised kitsendavad tingimused:

- Häälel peab olema üks ja ainult üks allkiri, mida hoitakse signatuurifailis `META-`

`INF/signature0.xml`;

- Kõik standardi poolt vormingu BES jaoks märgendiga M tähistatud elemendid tuleb valijarakenduses luua;
- Mitte ühtegi standardi poolt vormingu BES jaoks märgendiga C tähistatud elementi ei tohi kasutada;
- Mitte ühtegi standardi poolt vormingu BES jaoks märgendiga N/A tähistatud elementi ei tohi kasutada;
- Standardi poolt vormingu BES jaoks märgendiga O tähistatud elementidest lisab valijarakendus BDOC-BES vormingus häälele elemendi `SigningTime` kontekstis `SignedSignatureProperties`.

Valijarakenduses Mobiil-ID'ga allkirjastamiseks ettevalmistatav hääl (`hääl-bdoc-mobid`) peab järgima kõiki BDOC-BES vormingu nõudeid, kuid signatuurifail `META-INF/signature0.xml` peab olema tühi. Allkirjastamise protsessi viib lõpuni kesksüsteem, mis algatab ka allkirjastamise valija mobiiltelefonis ning vormistab elektroonilise hääle koos sertifikaadi allkirjastamisaegset kehtivust tagava kehtivuskinnitusega (`kehtivuskinnitus`). Kehtivuskinnitus esitatakse standardis RFC2560 [OCSP] defineeritud ASN.1 andmestruktuurina `OCSPResponse` ning seostatakse häälega vastavalt BDOC2.1 standardikavandile. Hääl (`hääl-bdoc`) talletatakse BDOC-TM vormingus.

BDOC-BES vormingus hääle (`hääl-bdoc-idcard`) korral pöördub kesksüsteem OCSP protokolli kasutades elektroonilise identiteedi taristu poole ning hangib kehtivuskinnituse (`kehtivuskinnitus`). Hääl ja kehtivuskinnitus seostatakse ning hääl (`hääl-bdoc`) talletatakse BDOC-TM vormingus.

Digitaalselt allkirjastatud häälele BDOC-TM vormingus on seatud järgmised kitsendavad tingimused:

- Hääl peab järgima kõiki BDOC-BES vormingus häälele seatud tingimusi;
- Kõik standardi poolt vormingu TM jaoks märgendiga M tähistatud elemendid tuleb kesksüsteemis luua;

```
hääl-bdoc-idcard = BDOC-BES (BDOC2.1)

hääl-bdoc-mobid = BDOC-BES (BDOC2.1)

hääl-bdoc = BDOC-TM (BDOC2.1)

kehtivuskinnitus = OCSPResponse (ASN.1, RFC2560)
```

Hääle allkirjastamisel tuleb kontrollida, et sertifikaadi kasutusvaldkonna piirangud ei keelaks sertifikaadi kasutamist elektrooniliseks hääletamiseks. Näiteks tehakse vahet riiklikult ja kommertsiaalselt väljastatud Mobiil-ID sertifikaatidel, lubades elektroonilisel hääletamisel osaleda vaid riiklikult väljastatud Mobiil-ID'ga. Vahe tegemine toimub sertifitseerimishierarhia ja vajadusel sertifitseerimispoliitikat identifitseeriva objekti-identifikaatori alusel.