Формат на електронните данни от машинното гласуване

Версия 1.6

Цел на документа

Целта на настоящият документ е да дефинира сигурен електронен формат на данните от машините за гласуване върху записващите технически устройства (ЗТУ).
Форматът обхваща резултатите от различните видове избори и възможността за разполагане на повече от една машина за гласуване в секция.

Кодификация на видовете избори

Видовете избори, произвеждани в България са описани в следната таблица, съдържаща константите, които ги идентифицират:

Константа Вид избор	Вид избор
1	Общински съвет
2	Кмет на община
4	Кмет на кметство
8	Кмет на район
16	Резервирано
32	Резервирано
64	Народно събрание
128	Членове на европейския парламент
256	Президент и вицепрезидент на Републиката

Общи изисквания за разполагане на информацията върху ЗТУ

Записващото техническо устройство на всяка машина за гласуване трябва да съдържа файл с данните в csv формат (описан детайлно по-долу) и файл, съдържащ електронния подпис на csv файла (.csv.p7s), създаден с една от контролните смарткарти (Член СИК 1 или Член СИК 2). Двата файла трябва да са разположени в root директорията на USB носителя върху NTFS/FAT32/FAT16 с LFN файлова система.
Ако в секцията се произвежда повече от един вид избор, информацията се записва в един общ файл, със съответния идентификатор за вид избор.
Ако за секцията са параметризирани повече от една машина за гласуване, то за втората и всяка следваща към единния номер на СИК се добавя *суфикс* с номер на машина, разделен с „-“ (ASCII код 0x2d), например:

```
Машина 1: 212000149
Машина 2: 212000149-1
Машина 3: 212000149-2
```

Изисквания към csv файла

- Име на файла с данните – номер на СИК[9 цифри] и в случай на разполагане на повече от една машина, суфикс(-1, -2 и т.н.), с разширение .csv

- Encoding – ASCII
- Край на редове - „\r\n“ (ASCII код 0x0d0a)
- Разделител - „;“ (ASCII код 0x3b)

Формат на съдържанието

Първият ред във файла трябва да съдържа информация за машината за гласуване и има следния вид:

`номер на СИК[9 цифри, опционално суфикс];криптографски hash на модулите на софтуера за гласуване;модел на МГ;идентификационен/сериен номер на машината за гласуване`

Криптографския hash на модулите на софтуера за гласуване е SHA-256 в hex кодиране, записан с малки или големи букви.

Полетата „модел на МГ“ и „идентификационен/сериен номер на машината за гласуване“ са буквено-цифрови с размерност до 256 байта.

Забележка 1:

При изчитане на данните криптографският hash ще бъде сравняван с официално потвърдения от одитиращите органи hash, като ако не съвпаднат, данните няма да бъдат приемани.

Пример:

```
212000149;3affd415bcd462927a838b944349ddf35abf4693bee09a05db53a673a3172047;ST124;38423843DVT1
```

Според вида избор, който се произвежда в съответната секция, съдържанието на следващите редове е както следва:

Вид избори „Общински съвет“, „Народно събрание“ и „Членове на европейския парламент“

`номер на СИК[9 цифри, опционално суфикс];константа за вид избор;номер по жребий на партия/коалиция от партии/инициативен комитет, регистриран в ЦИК/РИК/ОИК(П/КП/ИК);общ брой действителни гласове от МГ за П/КП/ИК;номер на кандидата в кандидатската листа, започващ от 101;брой на предпочитанията за кандидата`

Специално значение 1 - „Не подкрепям никого“:

`номер на СИК[9 цифри, опционално суфикс];константа за вид избор;`**`99;`**`брой „Не подкрепям никого“ в секцията;`**`0;0`**

Специално значение 2 - „Инициативни комитети“:

`номер на СИК[9 цифри, опционално суфикс];константа за вид избор;номер по жребий на ИК;брой действителни гласове за ИК в секцията;`**`0;0`**

Специално значение 3 – „Гласуване извън станата“:

При произвеждане на избори за народно събрание извън страната в случай, че няма мандати и съответно кандидатски листи за района, в полетата „номер на кандидата в кандидатската листа“ и „брой предпочитания за кандидата“ се записва „0“

`номер на СИК[9 цифри, опционално суфикс];константа за вид избор;номер по жребий на П/КП;брой действителни гласове за П/КП в секцията;`**`0;0`**

Забележка 1:

Във файла трябва да присъства информация за всички регистрирани П/КП/ИК и издигнатите от тях

кандидати и „Не подкрепям никого“, дори и да имат нула гласа

Забележка 2:
Броят на преференциите за различните кандидати се подава спрямо реално подадените преференции от гласоподавателите, без прибавяне на „без преференция“ към първия кандидат. В случай, че в даден избирателен район няма издигнати кандидати за регистрирана в ЦИК партия/коалиция от партии, то в полетата за номер на кандидат и предпочитания за кандидата се записва „0“.

Пример 212000149.csv

```
212000149;64;1;123;101;100
212000149;64;1;123;102;3
212000149;64;1;123;103;0
212000149;64;2;234;101;23
212000149;64;2;234;102;12
.........................
212000149;64;23;15;0;0
.........................
212000149;64;99;1;0;0
```

Контроли:

1. Каноничната част от името на файла (номер на СИК, опционално суфикс) трябва да съвпада с номера на СИК в колона 1 от файла;
2. Допустимите стойности в колона 2 от файла са „1“, „64“ и „128“;
3. Допустимите стойности в колона 3 от файла са номерата, изтеглени по жребий за П/КП/ИК, както и служебното „99“;
4. За една и съща стойност в колона 3 (номер на П/КП/ИК/“не подкрепям никого“) стойностите в колона 4 (общ брой действителни гласове в секцията за П/КП/ИК) трябва да съвпадат;
5. За една и съща стойност в колона 3 (номер на П/КП) сумата на числата в колона 6 (брой на предпочитанията за кандидата) трябва да бъде по-малка или равна на стойността в колона 4 (общ брой действителни гласове в секцията за П/КП);
6. Стойностите в колона 3 трябва да отговарят на номера на П/КП/ИК според изтегления от ЦИК/ОИК жребий;
7. В случай, че във файлът е налична информация за заличен кандидат, то предпочитанията за него се игнорират.

Вид избори „Кмет на община“, „Кмет на район“ „Кмет на кметство“ и „Президент и вицепрезидент на Републиката“

номер на СИК[9 цифри, опционално суфикс];константа за вид избор;номер по жребий на кандидат/кандидатска двойка, регистриран в ЦИК/ОИК(К/КД);общ брой действителни гласове от МГ за К/КД;код по ЕКАТТЕ на населеното място/района

Специално значение 1 - „Не подкрепям никого“:

номер на СИК[9 цифри, опционално суфикс];константа за вид избор;**99**;брой „Не подкрепям никого“ в секцията;код по ЕКАТТЕ на населеното място/района

Специално значение 2 - „Населено място/район“:

За вид избор 2 - „Кмет на община“ - в поле „код по ЕКАТТЕ на населеното място/района“ се записва ЕКАТТЕ кода на общината
За вид избор 4 - „Кмет на кметство“ - в поле „код по ЕКАТТЕ на населеното място/района“ се записва ЕКАТТЕ кода на кметството
За вид избор 8 - „Кмет на район“ - в поле „код по ЕКАТТЕ на населеното място/района“ се записва ЕКАТТЕ кода на района
За вид избор 256 - „Президент и вицепрезидент на Републиката“ - в поле „код по ЕКАТТЕ на населеното място/района“ се записва „0“

Забележка 1:
Във файла трябва да присъства информация за всички регистрирани К/КД и „Не подкрепям никого“, дори и да имат нула гласа

Пример 212000149.csv

```
212000149;4;1;123;69986
212000149;4;2;234;69986
212000149;4;3;21;69986
.........................
212000149;4;99;3;69986
```

Контроли:

1. Каноничната част от името на файла (номер на СИК, опционално суфикс) трябва да съвпада с номера на СИК в колона 1 от файла;
2. Допустимите стойности в колона 2 от файла са „2“, „4“, „8“ и „256“;
3. Допустимите стойности в колона 3 от файла са номерата, изтеглени по жребий за К/КД, както и служебното „99“;
4. За един и същ вид избор (колона 2) стойностите за код по ЕКАТТЕ на населеното място/района (колона 5) трябва да съвпадат
5. Стойностите в колона 3 трябва да отговарят на номера на П/КП/ИК според изтегления от ЦИК жребий;
6. В случай, че във файлът е налична информация за заличен кандидат, то предпочитанията за него се игнорират.

Изисквания към csv.p7s файла

1. Име на файла с електронният подпис – номер на СИК[9 цифри, опционално суфикс] с разширение .csv.p7s;
2. Формат – PKCS#7 detached signature, base64 encoded (PEM)

Електронно подписване

За подписване се използва една от двете контролни СИК (Член СИК 1/Член СИК 2) смарткарти, като номера на секцията в сертификата на смарткартата трябва да съвпада с номера на секцията, от която са данните, включително и суфиксът, ако има такъв. Типа на ключа за подписване трябва да бъде RSA с дължина 2048bit, а алгоритъмът за подписване на данните SHA256withRSA.
Необходимо е да се извършат интеграционни тестове за успешното изчитане и верифициране на трансферните файлове от контролните памети.