ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

Предмет на настоящата техническа спецификация е провеждането на процедура за обществена поръчка относно дейности по осигуряване на машинното гласуване в страната в изборите за общински съветници и за кметове на 29 октомври 2023 г. при произвеждане на първи и евентуално втори тур, както следва:

Дейност 1: Надграждане на системен и приложен софтуер за специализирани устройства за електронно машинно гласуване (СУЕМГ), в това число подготовка на демоверсия за обучение.

Изпълнителят трябва да надгради софтуера за работа на СУЕМГ за избор в два тура, в съответствие с актуализираните изисквания с промените в Изборния кодекс, публикувани в ДВ, бр. 104 от 30.12.2022 г. Техническите изисквания към СУЕМГ са детайлизирани в Приложение 1 към настоящия документ.

Резултатите от изпълнението на дейността са следните:

1. Актуален системен и приложен софтуер за многократна еднотипна работа в съответствие с техническите изисквания и адаптиран към спецификата на избор за общински съветници и за кметове на първи и втори тур с включена възможност за преференциален вот за общински съветници.

2. Актуален демонстрационен софтуер за нуждите на обучителната и разяснителната кампании, адаптиран към спецификата на избор за общински съветници и за кметове в два тура.

3. Изготвени без достъп до интернет и електронно подписани с UEFI ключ от ЦИК (елемент от софтуера, генериран в процеса на доверено изграждане защитен по подходящ начин от поне две нива за достъп), цифрови образи за инсталация на СУЕМГ. При изпълнение на т. 3 следва да бъде осигурена и възможност за цялостно администриране на СУЕМГ, вкл. и с достъп до настройки на периферията и портовете на базово софтуерно ниво. Като резултат цифровите образи следва да съдържат уникален хеш-код, който да удостоверява цифрово уникалността и единствеността на образите.

4. Изготвени инструкции за инсталиране и експлоатация, както и други документи в съответствие с Техническите изисквания.

Дейност 2: Параметризиращ софтуер за специализирани устройства за електронно машинно гласуване (СУЕМГ) с инсталиран софтуер по Дейност 1.

Резултатите от изпълнението на Дейност 2 са следните:

1. Параметризиращ софтуер за специализирани устройства за електронно машинно гласуване за многократно използване, позволяващ създаването на бюлетини от машинно гласуване, вкл. в два тура.

2. Инструкции за ползване на параметризиращия софтуер по т.1.

3. Параметризиране на данните за секциите, в които ще се произвежда машинно гласуване на първи и втори тур.

4. Параметризиране на бюлетините за гласуване за първи и втори тур.

5. Параметризиране на предоставените от ЦИК CA-вериги и информация за издадените смарткарти за управление и гласуване.

6. Изготвени и електронно подписани с UEFI ключ от ЦИК записани цифрови образи с изчислени хеш-суми на данните за параметризация на СУЕМГ за първи и втори тур. При това е необходимо подписаните образи да съдържат и резултантен хеш-код, различен от този по Дейност 1. Допуска се комбинирането на втория хеш-код с този за параметризация, като така се цели уникален хеш-код за всяко СУЕМГ. Новополученият хеш-код служи за служебни цели при възникване на технически въпроси. Публично се анонсира и публикува само хеш-кодът от довереното изграждане на софтуера за СУЕМГ.

7. Изготвени инструкции за параметризация на СУЕМГ, както и други документи в съответствие с Техническите изисквания.

8. Като резултат след инсталацията и параметризацията по Дейност 1 и Дейност 2 СУЕМГ следва да могат да отпечатват 4 различни бюлетини, начални и финални обобщени отчети с различна дължина (за по-лесна сортировка и контрол при броенето). Резултатите от гласуването следва да се съхраняват в идентичен, защитен вид и на преносими флаш-памети (2 бр. цифрово подписани със смарткартите на СИК с възможност за допълнително подписване за повишаване на сигурността с UEFI ключ от ЦИК) за контрол при броенето. Данните от работата на СУЕМГ следва да се записват в отделен лог-файл, който да може да бъде извлечен с лог-екстрактор и да послужи при евентуална проверка. За последващо извличане на данните от паметта на СУЕМГ следва да бъде предложен и подходящ инструмент, резултат от Дейност 1 и Дейност 2, както следва: хеш-екстрактор, лог-екстрактор и екстрактор на журналното съдържание и конфигурация на СУЕМГ.

Изпълнителят следва да представи в предложението си концепция за архитектура, интерфейс, надеждност, функционалност и електронна сигурност на приложния софтуер за СУЕМГ.

Изпълнителят следва да представи в предложението си за изпълнение екип за изпълнение на дейността с конкретно посочване на специалисти, притежаващи квалификация по отношение на използваните в България машини за гласуване (СУЕМГ) А-4 Модел 517 във връзка с Дейност 1 и Дейност 2. Изпълнителят следва да предостави документи (копия договори, актуални извлечения от плащания или други документи със заличени финансови данни), които доказват, че предложените поименни специалисти са в съответните договорни отношения с компанията.

След приключване на работата по Дейност 1, Изпълнителя инсталира и параметризира до 15 машини с удостоверения софтуер върху СУЕМГ, предоставени от ЦИК за целите на контрола на качеството, и демонстрира пред представители на ЦИК резултатите. След одобрение се подготвя пакет с актуалния програмен и изходен код по Дейност 1 и Дейност 2, както и детайлни инструкции за изграждането му, който се предава за удостоверяване. За Дейност 2 следва да се използва демонстрационен вариант за формата на бюлетината за гласуване.

Изпълнителят следва да окаже пълно съдействие на участниците в процеса на удостоверяване и да извърши корекции в СУЕМГ в този процес.

При успешно приключване на процеса изпълнителят съдейства за подписването на изградения и удостоверен образ с UEFI ключ на ЦИК (елемент от софтуера, генериран и защитен по подходящ начин от поне две нива за достъп), който позволява зареждането и изпълнението на новия удостоверен електронен образ върху машините за гласуване, което да става само за инсталационни носители, подписани от Възложителя.

Изпълнителят е длъжен да окаже съдействие на екипите, изпълняващи дейностите по подготовка, инсталиране и окомплектоване на СУЕМГ в склада за тях. Изпълнителят оказва техническа помощ и съдействие, подготвя мутимедийни и визулани обучителни материали за машинното гласуване.

ИЗПЪЛНИТЕЛЯТ трябва да представи в техническото предложение за одобрение от ЦИК не по-малко от два идейно различни варианта на интерфейса към визуализацията на бюлетините, които да дават на избирателя възможност да упражни правото си на глас на всички или на част от изборите за общински съвет, за кмет на община, за кмет на кметство или за кмет на район, като има възможност за промяна на избора си. При това трябва да е налице възможност за различим печат за всеки избор, който да позволява лесна сортировка на бюлетините. Пропускането на даден избор също трябва да бъде възможно с опцията „Пропусни“.

Участникът следва да отговаря на посочените по-долу критерии за подбор и изисквания за изпълнение:

- да прилага система за управление на качеството, съответстваща на стандарт БДС ЕN ISO 9001:2015 или еквивалентен с обхват, приложим към предмета на поръчката, или да представи доказателства за еквивалентни мерки. Под обхват, приложим към предмета на поръчката, се разбира: внедряване и поддръжка на софтуер за специализирани информационни системи и търговия с IT продукти;

- да прилага система за управление на сигурността на информацията, съответстваща на стандарт БДС EN ISO/IEC 27001 и система за управление на услугите, съответстваща на стандарти ISO/IEC 20000-1:2018, ISO/IEC 20000-2:2019 или еквивалентни, с обхват: внедряване и поддръжка на софтуер за специализирани информационни системи и търговия с IT продукти.

Препоръчителен срок за изпълнение за двете дейности – 30.09.2023 г. Сроковете по дейност 1 и дейност 2 подлежат на договаряне при провеждане на преговорите, като същите ще бъдат посочени в договора.

Техническата спецификация е неразделна част към Решение № 2438-МИ от 15.09.2023 г. на ЦИК.

Приложение № 1 към

Решение № 2438-МИ от

15.09.2023 г. на ЦИК

**Технически изисквания към СУЕМГ**

В съответствие с Изборния кодекс Централната избирателна комисия определя технически изисквания към апаратната и програмна част на специализираните устройства за електронно машинно гласуване.

1. Въведение

Общите изисквания към апаратната и програмна част на електронната система за машинно гласуване са дефинирани в чл. 213, ал. 2 от Изборния кодекс (ИК)

2. Общи изисквания

2.1. Изготвяне на електронни бюлетини за произвеждане на избори за общински съветници и за кметове на 29 октомври 2023 г. по образци, предоставени от ЦИК. Генерираните от СУЕМГ файлове да са в съответствие с утвърдена от ЦИК версия на формата за данните от машинно гласуване съгласно Приложение № 1.1

2.2. Създаване и удостоверяване на цифров образ, съдържащ комплект от операционна система, необходимите за изборния процес приложения, електронни бюлетини и конфигурации, съвместим с процеса на първоначално зареждане на СУЕМГ (Secure Bootable UEFI image), включително необходимите за това сертификати, с валидност не по-малка от срока на договора. Комплектът софтуер за СУЕМГ (Secure bootable UEFI image) трябва да бъде цифрово подписан с електронен подпис и с добавено квалифицирано удостоверение за времеви печат (Time stamp), издадено от доставчик на квалифицирани удостоверителни услуги в Република България, сертифициран съгласно изискванията на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни транзакции на вътрешния пазар и за отмяна на Директива 1999/93/ ЕО. Доставчикът на квалифицирани удостоверителни услуги, издал квалифицираното удостоверение за времеви печат, следва да е вписан в общият Европейски доверителен списък (European Union Trusted Lists).

2.3. Описание на техническите дневници (журнали) на машините (log files, results logs), необходими за проверка работоспособността на системите, както и за отчитане на грешки или разследване на инциденти, в това число и описание на 2D баркода, отпечатван на бюлетините от машинното гласуване;

2.4. В случаите, когато се използват криптографски механизми на защита на софтуера или се предават криптирани или защитени с парола данни и файлове, Изпълнителят предава паролите, ПИН-овете за достъп до тях и хеш-кодовете им на ЦИК, не по-късно от 1 работен ден след датата на удостоверяване.

2.5. Процедура и средства за точно отчитане на резултатите от изборния ден на всички възможни нива.

2.6. Предоставяне на обновени версии на firmware, базовия системен и конфигурационния софтуер, конфигурационни данни и документацията (вкл. инсталационна процедура и първичен инсталационен носител).

2.7. Подробна техническа документация за процесите за инсталация, конфигурация и персонализация на устройствата СУЕМГ.

3. Изпълнителят използва система за управление на риска чрез споделено изпълнение (peer-review) за всяка важна технологична операция при подготовката на софтуера, да бъде изпълнявана от двама участника (един от изпълнителя и един от възложителя).

4. Машините за гласуване трябва да поддържат машинен метод за импорт/експорт на конфигурации от ЕМР и входно-изходните данни да бъдат предадени на ЦИК до 2 работни дни след тяхното генериране.

5. Изходният формат на CSV файла за отчитане на резултатите от гласуване върху записващите технически устройства (ЗТУ) трябва бъде съгласно спецификация Формат на електронните данни от машинното гласуване – Приложение № 1.1.

6. Общо описание на процесите за машинно гласуване

6.1. Подготовка на системата. Извършва се на стъпки, както следва:

6.1.1. Параметризиране на механизма за защита на машината от злонамерено модифициране на софтуерните компоненти на машините по време на транспорт, генериране на ключ за криптиране, който ще бъде използван за full disk криптиране на дисковите образи на всяка една от СУЕМГ;

6.1.2. Изпълнителят ще получи от ЦИК персонализирани за съответните СИК смарткарти за гласуване и управление, включително и в електронен вид случайно генерирани ПИН-кодове за достъп. За всяка машина за гласуване ще бъдат налични 5 бр. смарткарти. Електронните сертификати върху смарткартите съдържат единствено пълния номер на секцията, в която ще се използват:

* 2 бр. смарткарти за управление: използват се от оторизираните членове на СИК за управление на машината по време на изборния ден и подписване на резултатите от гласуването с машината. ПИН-кодовете за тези карти се запечатват в непрозрачен плик и се предоставят на съответната СИК. В смарт картите за управление трябва да се запише и сигурен обект, съдържащ ключа за full disk криптирането (в случай че този подход се прилага от Изпълнителя).
* 3 бр. смарткарти за гласуване: използват се oт избирателите за отключване на СУЕМГ и подписване на електроните бюлетини, в случай че този подход се прилага от Изпълнителя. ПИН-кодовете за тези смарткарти се съхраняват в сигурна база данни.

6.1.3. Създаване на системен криптографски ключ (системен сертификат) подписан от СА-веригата (електронни подписи от ЦИК). С него ще бъдат подписвани номенклатурните данни и софтуерът за извършване на гласуването. Ако асиметричната ключова двойка се създава извън специализирано хардуерно устройство (смарткарта, HSM), частният ключ на ключовата двойка се разпределя по key escrow схема М of N между членовете на ЦИК с оглед възстановяване при евентуална загуба и използването му;

6.1.4. Подготовка на цифров базов образ (image) на операционната система и базовия системен софтуер за машинно електронно гласуване – инсталация на избраната операционна система, обновяване на компонентите и премахване на всички несвързани с работата на системата за гласуване нейни компоненти/драйвери/firmware образи. В базовия образ се добавя публичната част на генерирания системен асиметричен криптографски ключ;

6.1.5. Криптиране на цифровия базов образ с ключа за full disk криптиране, в случай че този подход се прилага от Изпълнителя. Резултатът е криптиран образ, който ще се използва за трансфер към всяка една машина за гласуване. Върху образа се изчислява уникален криптографски хеш, който се проверява преди всяка една инсталация.

1. Изисквания към софтуерната реализация и конфигурация
   1. Операционна система

Използваната операционна система трябва да бъде в поддръжка от производителя и максимално актуализирана с последните налични, надеждни кръпки (patches/service packs) за сигурност. Драйвери, модули и функционалности на операционната система, които нямат пряко отношение към машинното гласуване, трябва да бъдат премахнати или изключени по гарантиран сигурен начин. Мрежовата подсистема трябва да бъде отстранена или изключена по гарантиран, доказано сигурен начин. Използва се технология за сигурно стартиране (secure boot) за гарантиране на автентичността на операционната система и зарежданите в нея компоненти.

При прилагането на подход за пълно криптиране на вътрешната памет (full disk encryption) следва да се гарантира невъзможността за промяна на базовата операционна система по време на съхранение или транспортиране. Ключът, който ще се използва, трябва да бъде различен за всеки избор. В случай че ИзпълнителяТ прилага алтернативен подход за гарантиране на сигурността при съхранение или транспортиране, то следва този подход да гарантира минимум същото ниво на сигурност.

Процесът на стартиране на СУЕМГ е, както следва:

* Зареждане на базовия цифров образ;
* Зареждане на криптографски ключ в оперативната памет от контролната памет или чрез използване на контролна смарткарта след въвеждане на ПИН-код, в случай че този подход се прилага от Изпълнителя;
* Отключване на full disk криптирането с криптографския ключ, в случай че този подход се прилага от Изпълнителя;
* Зареждане на операционната система;
* Извършване на тест за наличие на необходимата периферия на СУЕМГ и състоянието на хардуерните компоненти;
* Извличане на софтуера за ЕМГ и/или параметризация от ЗТУ;
* Верифициране на електронния подпис на софтуера за ЕМГ;
* При успешна верификация софтуерът за ЕМГ се копира в основната памет на машината за гласуване;
* Стартиране на софтуера за ЕМГ. След стартиране на софтуера за ЕМГ системата изисква активиране със смарткарта за управление или гласуване. Изваждането на смарткартата автоматично заключва системата и я поставя в режим на изчакване.
  1. Първоначално стартиране

При първоначално стартиране на софтуера за ЕМГ се извършват следните действия:

* + 1. Проверява се за наличие на номенклатурни данни за произвежданите избори;
    2. Верификация на електронния подпис на номенклатурните данни. При успешна верификация данните се зареждат в системата за ЕМГ;
    3. Проверява се за наличие на валидни електронни бюлетини за тази избирателна секция – ако такива са налични и електронния им подпис е валиден, те се добавят в системата, а това се отбелязва в лог-файла на СУЕМГ;
    4. Софтуерът за ЕМГ визуализира екран за поставяне на смарткарта за управление.
    5. Действия за стартиране на гласуването:
    6. Член на СИК поставя смарткартите за гласуване една след друга в машината за гласуване. Системата визуализира номера на избирателната секция и извършва тестово електронно подписване чрез сертификата на картата и извършва верификация на подписа. По този начин се гарантира работоспособността на картите за гласуване;
    7. Член на СИК поставя една от смарткартите за управление;
    8. Въвежда валиден ПИН-код чрез сензорния екран или специализирано хардуерно устройство;
    9. Системата предоставя следния избор:
* Визуализация на параметризацията: визуализира се с възможност за разпечатване наличната параметризация на изборите в системата и статуса на вътрешния тест на периферните устройства. Вътрешният тест включва минимум идентифициране на наличие на хартия в принтера, наличие на ЗТУ, обем на свободната оперативна, контролна и вътрешна памет, резултат от верификацията на софтуера за ЕМГ и номенклатурните данни;
* Начало на гласуването – разпечатва наличната параметризация на изборите в системата, както и статуса на вътрешния тест на периферните устройства. Стартира гласуването в секцията;
* Изключване на машината за гласуване.
  1. Функционалност и гласуване чрез системата за ЕМГ по време на изборния ден – системата за ЕМГ трябва да визуализира и работи с четири вида бюлетини според конфигурацията на съответния избор:
     1. Бюлетина с избор на партия/коалиция/независим кандидат/„Не подкрепям никого“ за избор на Общински съвет.
     2. Бюлетина с избор на партия/коалиция/независим кандидат/„Не подкрепям никого“ за избор на Кмет на община.
     3. Бюлетина с избор на партия/коалиция/независим кандидат/„Не подкрепям никого“ за избор на Кмет на кметство.
     4. Бюлетина с избор на партия/коалиция/независим кандидат/„Не подкрепям никого“ за избор на Кмет на район.

Визуализацията на бюлетините за позициите от т.7.3.1 – 7.3.4 чрез следния интерфейс:

А. Бюлетините се визуализират последователно: на първия екран се визуализира бюлетината от т. 7.3.1 с бутон в горния край на екрана „Пропусни“ и в бутон в долния край на екрана „Гласуване“. На следващите екрани се визуализират последователно бюлетините от т. 7.3.2 – 7.3.4 с бутони в долния край на екрана „Гласувай“ и „Пропусни“. На всеки от втори и трети екран има и бутони „Предходен екран“ и „Следващ екран“, чрез които избирателя да прелиства визуализираните бюлетини. На първи екран има само бутон На последния екран вместо бутон „Следващ екран“, а на последния екран - бутони „Предходен екран” и „Край на гласуването“. Освен „Пропусни“, избирателя трябва да има възможност да избере „Не подкрепям никого“, както и съответни преференции при наличие за останалите изборни варианти.

Б. Началният екран съдържа меню за избор на вид бюлетина: с по един бутон за всяка от т. 7.3.1-7.3.4, и бутон „Край на гласуването“. При избор на съответния бутон се визуализира екран с бюлетината, отговаряща на избрания вид избори, с бутони „Гласувай“ и „Връщане в основното меню“ (начален екран с възможност за избиране на друг вид избор) в долния край на екрана.

Не се допуска „изрязване“ на текстовете в бюлетините.

При избор на втори тур се визуализират само позициите от т. 7.3.1 – 7.3.4, за които се провежда втори тур на изборите в съответната избирателна секция.

За осигуряване на достъпност от избиратели с намалено зрение системата трябва да предоставя висококонтрастен интерфейс за гласуване, възможност за увеличаване (zoom) или друг утвърден подход.

Необходимо е да бъдат заложени шрифтове Arial или Tahoma. които са доказано най-подходящи за хора с остатъчно зрение, както и да е заложена опцията „Bold“, с цел допълнително увеличаване четивността на текста.

Избирателите могат да направят своя избор в съответната бюлетина или да изберат „Не подкрепям никого“.

* 1. Използване на системата от избирател:
* Избирателят получава една от смарткартите за гласуване, която не е била използвана при последното гласуване;
* Избирателят поставя смарткартата в машината за гласуване и ако тя е разпозната, се визуализира началният екран за гласуване, одобрен от Възложителя;
* Системата за ЕМГ визуализира електронна бюлетина във вид, максимално близък до хартиената. В случай че бюлетината е с дължина по-голяма от вертикала на дисплея, интерфейсът предлага възможност за визуализация на следваща страница чрез визуални елементи (бутони) за прелистване, без използване на скролинг;

А. На първия екран се визуализира бюлетината от т. 7.3.1., избирателят отбелязва своя избор в съответните полета на електронната бюлетина и избира бутон в долния край на екрана „Гласуване”. Системата визуализира направения избор и изчаква потвърждение или дава възможност за връщане назад. При потвърждение, гласът на избирателя се отчита, автоматично се зарежда следващият екран с бюлетина за следващия вид избор, а екранът на направения вече избор става неактивен (може да се разглежда, но не и променя). Ако избирателят избере бутона в горния край на екрана „Пропусни”, се преминава на следващата страница, като екранът остава активен, т.е. избирателят може да се върне на него и да гласува. На следващите екрани се визуализират последователно бюлетините от т. 7.3.2 – 7.3.4 и се гласува по същия начин. С бутони „Предходен екран“ и „Следващ екран“ избирателят може да прелиства визуализираните бюлетини. След като избирателят е направил своя избор във всички видове избори, натиска бутон „Край на гласуването”.

Б. Началният екран съдържа меню за избор на вид бюлетина – с по един бутон за всяка от т. 7.3.1 – 7.3.4 и бутон „Край на гласуването“. При избор на съответния бутон се визуализира екран с бюлетината, отговаряща на избрания вид избори, с бутони „Гласувай“ и „Връщане в основното меню“ (начален екран с възможност за избиране на друг вид избор) в долния край на екрана. Избирателят отбелязва своя избор. Системата визуализира направения избор и изчаква потвърждение или дава възможност за връщане назад. Избирателят потвърждава направения избор. При потвърждаване системата се връща на първоначалното меню, като бутонът на вече направения избор става неактивен.

* Системата подписва направения избор със сертификата на смарткарта за гласуване или с вътрешен за машината сертификат и записва електронната бюлетина във вътрешната памет и на ЗТУ. Софтуерът за ЕМГ експлицитно извършва записване на буферите на паметите (fsync или използване на пряк запис /DirectIO/). Записът се извършва по такъв начин, че да не може да се установи поредност на подаване на гласовете и индивидуализиране на избирателя;
* След като избирателят е гласувал за всички видове избори, за които желае (натиснал е бутон „Край на гласуването“), машината разпечатва бюлетина за всеки един от тях, съдържаща в текстови четим вид пълния номер на избирателната секция; идентификационния номер на машината; избора, в който ще се гласува; избраната партия/коалиция/независим кандидат или „Не подкрепям никого“, избран кандидат с предпочитание, както и системния хеш код на софтуера. Същата информация се разполага и в 2D баркод; дължината на бюлетината е различна за различна за избор на общински съветници, на кмет на община, на кмет на кметство и на кмет на район.
* Избирателят взима разпечатаните бюлетини и смарткартата. Бюлетината се сгъва по начин, недопускащ разкриване на вота, подпечатва се от член на СИК и се пуска в специалната кутия за машинното гласуване, а смарткартата за гласуване се връща на СИК.
  1. Използване на системата от СИК:
* Член на СИК поставя една от смарткартите за управление;
* Въвежда валиден ПИН-код чрез сензорния екран на СУЕМГ или специализирано хардуерно устройство;
* Системата визуализира броя на гласувалите чрез ЕМГ до момента;
* Системата предоставя следния избор:
* Край на гласуването – приключване на изборния ден. Системата изисква въвеждане на ПИН за потвърждение:
* Изключване на машината за гласуване.
* Ако не е избрано „Край на гласуването“ или машината не е изключена, при изваждане на смарткартата за управление машината за гласуване се връща в нормален режим на работа, при който се очаква включване на смарткарта за гласуване. Функционалност на системата за ЕМГ след края на изборния ден. След като гласуването е приключило, системата за ЕМГ трябва да предоставя следните възможности:
* Член на СИК поставя една от смарткартите за управление;
* Въвежда валиден ПИН-код чрез сензорния екран или специализирано хардуерно устройство:
* Системата визуализира броя на гласувалите чрез ЕМГ до момента и предоставя избор за изключване на машината за гласуване.
  1. **Модул за валидация и обобщаване**

Изпълнителят трябва да предостави софтуерен модул, чрез който да се разпознава 2D баркодът, отпечатван на бюлетината от машината, и да се обобщават данните в рамките на избирателна секция. Минималната информация в баркода трябва да включва:

* Пълен номер на избирателната секция.
* Идентификационен номер на машината за гласуване.
* Вид избор, за който е бюлетината.
* Направен избор от избирателя.
* Уникален номер на бюлетината.
* Хеш код на софтуера.

При наличие на електронни бюлетини от основната и/или контролните памети на машината за гласуване трябва да има възможност за сравняване на електронните бюлетини и отпечатаните бюлетини по уникалния им номер, което ще потвърди автентичността на отпечатаната от машината за гласуване бюлетина.

1. Изисквания към сигурността на устройствата за ЕМГ
   1. Общи изисквания
      1. Минимални изисквания към прилаганите криптографски алгоритми

* За криптографските хеш функции – SHA-256 или еквивалентни;
* За симетричните криптографски алгоритми – AES-256 или еквивалентни;
* За асиметричните криптографски алгоритми – RSA 2048 bit, ECC-256 bit или еквивалентни
  1. Изисквания към конфигурацията на операционната система
* Всички процеси, част от операционната система, които нямат отношение към системата за ЕМГ, трябва да бъдат премахнати;
* Всички firmware пакети и драйвери, управляващи хардуерни подсистеми, които нямат отношение към системата за ЕМГ, трябва да бъдат премахнати;
* Цялата комуникационна подсистема, обслужваща различните комуникационни протоколи (жични и безжични), трябва да бъде премахната.
  1. Изисквания към софтуерната реализация
     1. Конфигурацията на процеса по компилиране и изграждане (compile & build) на софтуера трябва да бъде реализирана и конфигурирана като репродуцируем процес (reproducable builds);
     2. Трябва да бъде предотвратена възможността за разкриване на вота чрез анализ на електронните log-ове:
        + чрез засичане на гласовете като последователност;
        + чрез засичане на гласовете по време на подаването им.

1. Процедури

Необходимо е да се предвидят подробни процедури и мерки за защита, а именно:

* Процедура за профилактика, тестване и калибриране на хардуера на машината за гласуване по стандартите на производителя;
* Оценка на необходимото време за изпълнение на процедурата по ЕМГ от един избирател за изборите за общински съветници и кметове;
* Подход за използване на повече от една машина за гласуване в една секция;
* Процедура по гарантиране анонимността на вота при предаване на отпечатаната от машината бюлетина на СИК за подпечатване и пускане в урната;
* Метод за предотвратяване на манипулирането на машинния вот от един избирател по време на тайния вот;
* Метод за предотвратяване на манипулирането на машинния вот от договорили се предварително двама или повече избиратели, включително да се предвиди защита на вота от отключване на машината от избирател, който не прави избор, и последващо двойно гласуване от следващ избирател;
* Метод за предотвратяване на манипулирането на машинния вот от страна на членовете на СИК.

Приложение № 1.1

Към Приложение № 1 към

Решение № 2438-МИ от

15.09.2023 г. на ЦИК

**Формат на електронните данни от машинното гласуване**

**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 (СУЕМГ) 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**

1. 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
2. Encoding – ASCII
3. Край на редове – „\r\n“ (ASCII код 0x0d0a)
4. 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.

Криптографският 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 страната“:

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:

* Каноничната част от името на файла (номер на СИК, опционално суфикс) трябва да съвпада с номера на СИК в колона 1 от файла;
* Допустимите стойности в колона 2 от файла са „1“, „64“ и „128“;
* Допустимите стойности в колона 3 от файла са номерата, изтеглени по жребий за П/КП/ИК, както и служебното „99“;
* 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;
* 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);
* Стойностите в колона 3 трябва да отговарят на номера на П/КП/ИК според изтегления от ЦИК жребий;
* 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:

* Каноничната част от името на файла (номер на СИК, опционално суфикс) трябва да съвпада с номера на СИК в колона 1 от файла;
* Допустимите стойности в колона 2 от файла са „2“, „4“, „8“ и „256“;
* Допустимите стойности в колона 3 от файла са номерата, изтеглени по жребий за К/КД, както и служебното „99“;
* За един и същ вид избор (колона 2) стойностите за код по ЕКАТТЕ на населеното място/района (колона 5) трябва да съвпадат
* Стойностите в колона 3 трябва да отговарят на номера на П/КП/ИК според изтегления от ЦИК жребий;
* 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 номерът на секцията в сертификата на смарткартата трябва да съвпада с номера на секцията, от която са данните, включително и суфиксът, ако има такъв. Типът 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.