**ПРИЛОЖЕНИЕ №4**

# Процедура за проверка на сигурността на информацията, която се въвежда, обработва, съхранява и извежда от ТУМГ

| **1. Проверка на хардуерната платформа** | | | | |
|---|---|---|---|---|
| **Действие** | **Очакван резултат/ Критерий за оценяване** | **Констатация /Забележка** | **Съответствие** | **Съответствие съгласно Техническата спецификация** |
| Проверка за наличие на възможност за комуникация през хардуерните интерфейси. | Установена липса или наличие на възможност за комуникация през хардуерните интерфейси на ТУМГ.<br>Установена липса или наличие на активни хардуерни интерфейси. | | | |
| Проверка за наличие на активни комуникационни интерфейси, вградени в ТУМГ. | Установена липса или наличие на възможност за комуникация през комуникационните интерфейси.<br>Установена липса или наличие на активни комуникационни интерфейси. | | | |
| Проверка за наличие на активна комуникационна подсистема. | Установена липса или наличие на възможност за комуникация чрез комуникационната подсистема./<br>Установена липса или наличие на активна комуникационна подсистема, обслужваща различните комуникационни протоколи. | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| Проверка за наличие на активни специализирани интерфейси. | Установена липса или наличие на възможност за комуникация през специализираните интерфейси.<br><br>Установена липса или наличие на активни специализирани интерфейси (микрофон/аудио изход/сериен порт/паралелен порт). | | | |
| **2. Проверка на конфигурацията на операционната система** | | | | |
| **Действие** | **Очакван резултат/ Критерий за оценяване** | **Констатация /Забележка** | **Съответствие** | **Съответствие съгласно Техническата спецификация** |
| Проверка дали софтуерни компоненти на операционната система на ТУМГ са актуализирани (спрямо последните публикувани варианти). | Установяване на версията на софтуерните компоненти на ТУМГ и дали са актуална версия с последни кръпки и обновления за уязвимости в текущата ОС, свързани със сигурността. | | | |
| Проверка дали са деактивирани ненужни процеси в операционната система на ТУМГ. | Предоставен от страна на Изпълнителя по Договора по обществената поръчка списък с всички процеси в операционната система, които имат отношение към системата на ТУМГ./Липса на процеси, част от операционната система на ТУМГ, които нямат отношение към системата на ТУМГ. | | | |

| | | | | |
|---|---|---|---|---|
| Проверка за премахнати ненужни firmware драйвери и модули в ядрото на ТУМГ. | Установяване на липса или наличие на firmware драйвери и модули в ядрото на ТУМГ, които управляват хардуерните подсистеми на ТУМГ, нямащи отношение към обезпечаване на изборния процес. | | | |
| Проверка за наличие на уязвимости в операционната система на ТУМГ. | Установена липса или наличие на уязвимости в операционната система на ТУМГ. | | | |
| Извършване на оценка за нивото на въздействие, при наличие на открити уязвимости в операционната система на ТУМГ, съгласно Common Vulnerability Scoring System v3.1 (CVSS 3.1) или еквивалентна схема. | Оценка на нивото на въздействие при открити уязвимости съгласно CVSS 3.1 (Common vulnerability scoring system) или еквивалентна система в ОС на ТУМГ. | | | |
| Подготовка на базов образ на операционната система и базовия софтуер за машинно електронно гласуване | | | | |
| **3. Проверка на софтуерната реализация на приложната информационна система** | | | | |
| **Действие** | **Очакван резултат/ Критерий за оценяване** | **Констатация /Забележка** | **Съответствие** | **Съответствие съгласно Техническата спецификация** |

| | | | | |
|---|---|---|---|---|
| Компилиране на изходния код на софтуера в специализирана среда. Тестване за наличието на зависимости в програмния код. | Програмен код със зависимостиот външен код или библиотеки, които не са предоставени или налични в средата.<br><br>Генерираният бинарен файл на софтуера за ТУМГ следва да бъде изпълним и оперативен повсички заложени критерии за функционалност след компилацията на изходния код в друга среда.<br><br>При предоставяне на чистаТУМГ и извършени всички действия по удостоверяване и проверка на код, и генериране на уникален системен криптографски идентификатор (хеш) след компилирането, чрез който се идентифицират произведените софтуерни компоненти, сравнено спрямо предварително известен или предоставен такъв идентификатор от ЦИК, както и методът/алгоритъм на хеширане. | | | |
| Проверка за наличие на уязвимости в приложния софтуер на ТУМГ. | Установяване на липса или на наличие на уязвимости в приложната информационна система на ТУМГ. | | | |

| | | | | |
|---|---|---|---|---|
| Проверка за възможност за разкриване на вота чрез анализ на данните, записани в електронната избирателна кутия. Проверка за непоследователно записване на подадените гласове. | Установяване на липса или наличие на данни, записани във файловете на електронната избирателна кутия, съдържащи идентификационна информация. (За идентификационна информация се считат времеви показатели като дата, час; уникални идентификатори - ID номера, на заявката и други показатели, които могат да идентифицират избирателя). Установяване на липса или наличие на механизъм за непоследователно записване на подадените. | | | |
| Проверка за наличие на обфускиран (прикрит) код, напр. кодиран с Base64 или друга популярна схема за кодиране | Проверка за наличие на обфускиран (прикрит) код на основни или избрани компоненти на приложния софтуер и софтуерни компоненти, обслужващи изходния код на ТУМГ, напр. кодиран с Base64 или друга популярна схема за кодиране, за съответствие с официално публикуваните от разработчика на операционната система за дадената версия. | | | |
| Проверка на базова/и СА верига/и, използвана/и при конкретните избори | Проверка на възможностите за компилация на изходния код, използвайки валиден, невалиден и изтекъл сертификат. | | | |

| | | | | |
|---|---|---|---|---|
| | При използване на валиден сертификат се очаква нормална компилация на изходния код и получаванена валидни резултати.<br><br>При използване на невалиден сертификат се очаква нормална компилация и получаване на невалидни резултати.<br><br>При използване на изтекъл сертификат се очаква изходния код да не може да се компилира. | | | |
| Детайлна проверка на предвиденото поведение на всички места в изходния код, които работят с файла или файловете за съхранение на гласове | Установяване на поведението на всички места в изходния код, където се работи с файла или файловете за съхранение на гласове.<br><br>Проверка на установеното поведение с предвиденото такова. | | | |
| Персонализиране на смарт карти за гласуване и управление | Инсталираните върху картите сертификати следва да бъдат част от базовата СА верига | Картите съдържат сертификати, в които има следните данни: № на секция и типа карта | | |
| **4. Проверка на софтуерната реализация на ТУМГ.** | | | | |
| **Действие** | **Очакван резултат/ Критерий за оценяване** | **Констатация /Забележка** | **Съответствие** | **Съответствие съгласно Техническата спецификация** |

| | | | | |
|---|---|---|---|---|
| Компилиране на изходния код на софтуера в специализирана среда. Тестване за наличието на зависимости в програмния код. Инсталиране и конфигуриране в специализирана среда. | Установено наличие на произведена и инсталирана софтуерна реализация на ТУМГ. | | | |
| Проверка на списък с определени методи и поетапно тестване по предефинирани критерии за съответствие. | Установено наличие на unit tests, които покриват 70% от изходния код на базовия софтуер. Генерирани >70% unit tests./Сравнени резултати от генерираните unit tests с предоставените. | | | |
| Проверка за наличие на уязвимости в ТУМГ. | Установена липса или наличие на уязвимости ТУМГ. | | | |
| Детайлна проверка на предвиденото поведение на всички места в изходния код, които работят с файла или файловете за съхранение на гласове. | Установяване на липса или наличие на отклонение в очакваното поведение на всички входни и изходни файлове, на очакваните места, които работят с файла или файловете за съхранение на гласове. | | | |
| Проверка на базова/и СА верига/и, използвана/и при конкретните избори. | Проверка на възможностите за компилация на изходния код, използвайки валиден, невалиден и изтекъл сертификат. | | | |

| | | | | |
|---|---|---|---|---|
| | При използване на валиден сертификат се очаква нормална компилация на изходния код и получаване на валидни резултати.<br><br>При използване на невалиден сертификат се очаква нормална компилация и получаване на невалидни резултати.<br><br>При използване на изтекъл сертификат се очаква изходния код да не може да се компилира. | | | |
| Проверка за сигурността на използваните криптографски механизми:<br><br>Хеш алгоритми – поне SHA-256<br><br>Симетрични алгоритми- поне AES -256<br><br>Асиметрични алгоритми – RSA 2048 | Всички използвани криптографски механизми покриват изискванията/ Установени са криптографски механизми, които не покриват изискванията. | | | |
| Проверка на шрифтове и функция bold | Наличие или липса на шрифтове Arial или Tahoma.<br><br>Наличие или липса на функцията bold. | | | |
| Проверка на заложената функционалност и обхвата на хешираните | Проверка на заложената функционалност и обхвата на хешираните файлове и | | | |

| | | | | |
|---|---|---|---|---|
| файлове и директории, участващите в приложението за проверка на хеш кода (HashExtractor). | директории, участващите в приложението за проверка на хеш кода (HashExtractor) включва, и заложената функционалност в приложението, след предоставяне на кода на HashExtractor-а. | | | |
| Детайлна проверка на предвиденото поведение на всички места в изходния код, които работят с файла или файловете за съхранение на гласове; | Проверка на предвиденото поведение на всички места в изходния код, които работят с файла или файловете за съхранение на гласове. | | | |
| Проверка за наличие на обфускиран (прикрит) код, в стандартните функционалности на операционната система. | Проверка за наличие на обфускиран (прикрит) код на основни или избрани компоненти на операционната система, напр. кодиран с Base64 или друга популярна схема за кодиране, за съответствие с официално публикуваните от разработчикана операционната система за дадената версия. | | | |