**ПРИЛОЖЕНИЕ №4**

**Проверка на сигурността на ТУМГ**

|  |
| --- |
| 1. **Проверка на криптографските механизми**
 |
| **Действие** | **Очакван резултат/ Критерий за оценяване**  | **Констатация /Забележка** | **Съответствие** | **Съответствие с техническата спецификация** |
| Удостоверяване от страна на вендора/доставчика за поддържаните криптографски алгоритми | Предоставени данни от вендора/доставчика доказват, че криптографските примитиви SHA-256, AES-256 и RSA-2048 се поддържат от софтуера на смарт картата |  |  | Т.2, ред 8 от таблицата стр 26;Т. 4.1 стр. 35 |
| 1. **Проверка на хардуерната система**
 |
| **Действие** | **Очакван резултат/ Критерий за оценяване**  | **Констатация /Забележка** | **Съответствие** | **Съответствие с техническата спецификация** |
| Защита на хардуерните интерфейси – машината за гласуване не трябва да излага незащитени интерфейси, извън монолитния корпус | Не трябва да бъдат открити незащитени хардуерни интерфейси извън монолитния корпус на ТУМГ |  |  | Т. 4.2, стр. 35 |
| Опит за достъп до физически интерфейси на машината без да бъде нарушена целостта на стикерите / пломбите | Нарушена цялост на стикери / пломби в случай на опит за физически достъп до интерфейс на ТУМГ |  |  | Т. 4.2, стр. 35 |
| Проверка за наличие на активни комуникационни интерфейси вградени в ТУМГ | Липса на комуникационни модули. В случай, че има комуникационни модули, те да бъдат деактивирани от базовата входно-изходна система (BIOS).  |  |  | Т. 4.2, стр. 35 |
| Проверка за наличие на вградени комуникационни антени в ТУМГ | Антените да са премахнати или прекъснати от комуникационните модули. |  |  | Т. 4.2, стр. 35 |
| Проверка дали цялата комуникационна подсистема, обслужваща различните комуникационни протоколи, е премахната. | Цялата комуникационна подсистема, обслужваща различните комуникационни протоколи, е премахната |  |  | Т. 4.2, стр. 35 |
| Проверка за наличие на специализирани интерфейси | В случай, че има специализирани интерфейси, те да са деактивирани от базовата входно-изходна система (BIOS) или да са физически прекъснати (например микрофон/аудио изход/сериен порт/паралелен порт). |  |  | Т. 4.2, стр. 35 |
| Проверка дали интерфейсите за контролните памети са осигурени чрез сигурно заключване или чрез сигурен стикер | Интерфейсите за контролните памети са осигурени чрез сигурно заключване или чрез сигурен стикер. |  |  | Т. 4.2, стр. 35 |
| Проверка за наличие на подвижни части в ТУМГ | Да не бъдат открити подвижни части в ТУМГ |  |  | Т. 4.2, стр. 35 |
| Проверка за електромагнитни излъчвания или протокол, че няма електромагнитни излъчвания, чрез които може да се идентифицира състоянието и данните, свързани с процеса на гласуване | При измерване да не бъдат установени електромагнитни излъчвания по време на процесите на гласуване, документирано в протокол от извършени изпитвания в Лаборатория за електромагнитна съвместимост на БИМ за обхвати 9kHz÷30MHz и 30MHz÷6GHz (8GHz). |  |  | Т. 4.2, стр. 35 |
| 1. **Проверка на конфигурацията на операционната система**
 |
| **Действие** | **Очакван резултат/ Критерий за оценяване**  | **Констатация /Забележка** | **Съответствие** | **Съответствие с техническата спецификация** |
| Всички процеси, част от операционната система, които нямат отношение към системата за ТУМГ трябва да бъдат премахнати | Да има предоставен от страна на вендора/доставчика списък с всички процеси, част от операционната система, които имат отношение към системата за ТУМГ.Да не бъдат открити процеси, част от операционната система, които нямат отношение към системата за ТУМГ |  |  | Т. 4.3, стр. 35 |
| Всички firmware пакети и драйвери, управляващи хардуерни подсистеми, които нямат отношение към системата за ТУМГ трябва да бъдат премахнати | Да има предоставен от страна на вендора/доставчика списък с всички firmware пакети и драйвери, управляващи хардуерни подсистеми, които имат отношение към системата за ТУМГ.Да не бъдат открити firmware пакети и драйвери, управляващи хардуерни подсистеми, които нямат отношение към системата за ТУМГ |  |  | Т. 4.3, стр. 35 |
| Тест за наличие на уязвимости в операционната система. | След провеждане на тест за уязвимост на операционната система на ТУМГ, да не бъдат установени критични уязвимости според Общата система за оценка на уязвимостите (CVSS). |  |  | Т. 4.3, стр. 35 |
| Проверка използваната операционна система дали е максимално актуализирана с последните налични кръпки (patches/service packs) за сигурността. | Използваната операционна система трябва да бъде максимално актуализирана с последните налични кръпки (patches/service packs) за сигурността. |  |  | Т. 3.1, стр. 31 |
| 1. **Проверка на софтуерната реализация**
 |
| **Действие** | **Очакван резултат/ Критерий за оценяване**  | **Констатация /Забележка** | **Съответствие** | **Съответствие с техническата спецификация** |
| Проверка на списък с всички налични методи и поетапно тестване по предефинирани критерии за съответствие. Сравняване на генерираните тестове с предоставените | Да са налични предоставени тестове, които трябва да представляват 70% или повече от генерираните тестове |  |  | Т. 4.4, стр. 35 |
| Компилиране на изходния код на софтуера в различна среда с цел тестване за наличието на зависимости в програмния код | Генерираният бинарен файл на софтуера за ТУМГ следва да бъде изпълним и оперативен по всички заложени критерии за функционалност след компилацията на изходния код в друга среда |  |  | Т. 4.4, стр. 35 |
| Тест за наличие на уязвимости в приложния софтуер. | След провеждане на тест за уязвимости на допълнителния софтуер инсталиран на ТУМГ, да не бъдат установени критични уязвимости според Общата система за оценка на уязвимостите (CVSS). |  |  | Т. 4.4, стр. 35 |
| Анализ на електронните лог файлове за наличие на възможност за разкриване на вота | Форматът на данните записани в електронните лог файлове не трябва да съдържат идентификационна информация. За идентификационна информация за считат времеви показатели (дата, час), уникални идентификатори (ID номера) на заявката и други показатели, които могат да идентифицират гласоподавателя |  |  | Т. 4.4, стр. 35 |