

**Процедура за проверка на сигурността на информацията, която се въвежда,
обработка, съхранява и извежда от ТУМГ**

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
1. Проверка на хардуерните компоненти на ТУМГ				
Проверка за наличие на възможност за комуникация през хардуерните интерфейси.	Установена липса или наличие на възможност за комуникация през хардуерните интерфейси на ТУМГ. 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. 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./			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
	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. Установена липса или наличие на активни специализирани интерфейси (микрофон/аудио изход/сериен порт/паралелен порт).			
2. Проверка на конфигурацията на операционната система				
Проверка дали софтуерни компоненти на операционната система на ТУМГ са актуализирани (спрямо последните публикувани актуални версии).	Установяване на версията на софтуерните компоненти на ТУМГ и дали са актуална версия с последни кърпки и обновления за уязвимости в текущата ОС, свързани със сигурността.			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
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 (ядрото и приложния слой на вградените компоненти) на ТУМГ.	Установена липса или наличие на уязвимости в операционната система (ядрото и приложния слой на вградените компоненти) на ТУМГ.			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
Извършване на оценка за нивото на въздействие, при наличие на открити уязвимости в операционната система (ядрото и приложния слой на вградените компоненти) на ТУМГ, съгласно Common Vulnerability Scoring System v3.1 (CVSS 3.1) или еквивалентна схема.	Оценка на нивото на въздействие при открити уязвимости в операционната система (ядрото и приложния слой на вградените компоненти), 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	Подготвен лаптоп с указаната операционна система от процедурата за изграждане, предоставена от ЦИК; копиране на изходния код, предоставен от ЦИК на работния лаптоп и проверка на валидиращи контролни суми, предоставени от ЦИК; изпълнено тестово изграждане - базов образ на Операционната система и приложен софтуер на ТУМГ от предоставения изходен код; Подготовка на 4 броя артефакти - зареждаща (bootable) флаш-памет за инсталация на ТУМГ от тестовото изграждане; флаш-памет за отключване на UEFI Bios (Unlocker); флаш-			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
	памет с Hash-extractor и флаш-памет с Log-extractor; Инсталиране на тестови ТУМГ за Екип 2, 3 и 4 за последващи тестове в процеса по удостоверяване.			
3. Проверка на софтуерната реализация на приложната информационна система				
Проверка на изходния код на софтуера в специализирана среда. Тестване за наличието на зависимости в програмния код.	Програмен код със зависимости от външен код или библиотеки, които не са предоставени или налични в дистрибутива или изходния код. Генерираният бинарен файл на софтуера за ТУМГ следва да бъде изпълним и оперативен по всички заложиени критерии за функционалност след компилацията на изходния код в друга среда. Извършване на всички действия по удостоверяване и проверка на код, и обследване на процеса по генериране на уникален системен криптографски			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
	идентификатор (хеш) след изграждането, чрез който се идентифицират тестовия образ на ТУМГ.			
Проверка за наличие на уязвимости в приложния софтуер на ТУМГ.	Установяване на липса или на наличие на уязвимости в приложната информационна система на ТУМГ чрез преглед и статичен анализ на кода, както и обследване на откритите находки посредством SAST аналитичен инструмент			
Въвеждане на тестови данни и проверка на параметризиращия софтуер, използван за подготовка на ТУМГ	Тестово въвеждане и настройка на данните, необходими за параметризация на ТУМГ; Установяване на наличие или липси на уязвимости в параметризиращия софтуер; Оценка на нивото на въздействие на евентуално открити уязвимости в параметризиращия софтуер съгласно CVSS 3.1. или по-висока версия.			
Проверка за възможност за разкриване на вота чрез анализ на данните,	Установяване на липса или наличие на данни, записани във файловете на електронната избирателна кутия,			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
записани в електронната избирателна кутия. Проверка за непоследователно записване на подадените гласове.	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 в софтуерната реализация на приложната информационна система	Проверка за наличие на обфускиран (прикрит) код на основни или избрани компоненти на приложната информационна система и нейните софтуерни компоненти, търсене по ентропия за непрозрачност и аномалии във функциите, 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 функциониране на ТУМГ, използвайки валидни разменени (от друга ТУМГ) и различни видове невалидни сертификати.			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
Детайлна проверка на въведените защитни механизми на всички места за съхранение на файловете, съдържащи гласове на избиратели	Установяване на въведените защитни механизми на местата за съхранение на файлове, съдържащи гласове на избиратели, в т.ч. надеждност, автентичност и интегритет.			
Проверка на смарт картите за гласуване и управление на изборния процес	Инсталираните върху картите сертификати следва да бъдат част от базовата СА верига на издателя, и ако не може да бъдат установени, да бъде извършена верификация на издадените сертификати чрез предоставена базова СА верига от издателя. Проверка на сертификатите за наличие на записи, които присвояват дадени карти към конкретна избирателна секция.			
Проверка за функционалност на HashExtractor при наличие или липса на USB block devices	Установяване на правилно функциониране на HashExtractor и визуализиране на очакван хеш резултат при наличие или липса на Smartmatic USB флаш-памети за съхранение на информация. Проверката установява дали правилно изчита Mass-block devices на ТУМГ с правилната локация за проверка на хеш сумата на базовия образ			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
Проверка за функционалност на генерираните четири артефакта (HashExtractor, Log-Extractor, Installer, Unlocker).	Установяване на правилно функциониране на артефактите.			
4. Проверка на софтуерната реализация на ТУМГ.				
Проверка на резултата от компилирането 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 и тестване за зависимости			
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.			

Действие	Очакван резултат/ Критерий за оценяване	Констатация /Забележка	Съответствие	Съответствие съгласно Техническата спецификация
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 софтуерната реализация на функциите за реализация на базова/и СА верига/и и сертификати в ТУМГ, в т.ч. присъединяване на сертификати към определена секция, подписване на протоколи, отключване на режим на гласуване и др.	Проверка на всички места в изходния код, където се използват сертификати за работата на ТУМГ. Валидиране на правилната работоспособност на сертификатите за последователност при избори, подписване на финализиращ протокол, активиране на диагностичен режим и режим за гласуване чрез персонализирани смарт карти.			

Проверка за сигурността на използваните криптографски механизми: Хеш алгоритми – минимум: - SHA-256 - Симетрични алгоритми- поне AES -256 - Асиметрични алгоритми – RSA 2048	Всички използвани криптографски механизми покриват изискванията/ Установени са криптографски механизми, които не покриват изискванията.			
Проверка на заложената функционалност и обхвата на приложението за проверка на хеш кода (HashExtractor).	Проверка на заложената функционалност и обхвата на визуализация на хеш кода: 1. Посредством флаш-памет HashExtractor; 2. заложената функционалност в приложението на ТУМГ и средствата за визуализирането им -за отпечатване на начални и крайни бюлетини, както и в диагностичното меню. Резултатът верифицира първоизточника на този хеш и при трите вида визуализация, като проверява за липса или наличие на предварително дефинирани (скрити) функции за манипулация на този хеш.			

Проверка за наличие на обфускиран (прикрит) код, в стандартните функционалности на софтуерната реализация на ТУМГ	Проверка за наличие на обфускиран (прикрит) код на основни или избрани компоненти на приложния софтуер и софтуерната реализация на ТУМГ, търсене по ентропия за непрозрачност и аномалии във функциите, 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.			
---	---	--	--	--