РУКОВОДСТВО ПО РАБОТЕ С ДОВЕРЕННОЙ СРЕДОЙ ИСПОЛНЕНИЯ АВРОРА

Версия 1.0

Листов 11

2025

АННОТАЦИЯ

Настоящий документ является руководством по работе с Доверенной средой исполнения Аврора (Аврора TEE).

Аврора TEE – изолированная от системы общего назначения (операционной системы (ОС) Аврора) среда для работы сервисов, к которым предъявляются повышенные требования безопасности (например, криптографические, финансовые сервисы или сервисы, работающие с персональными данными).

Основной целью применения Аврора TEE является обеспечение изолированной вычислительной среды для повышения безопасности при работе с критическими данными (например, персональными), а также защита таких данных при хранении криптографическими, либо аппаратными методами.

Взаимодействие с сервисами осуществляют приложения из состава ОС Аврора посредством программного интерфейса, то есть обращаются к функциям доверенных приложений (сервисов) и получают результат их выполнения.

Перед началом работы необходимо ознакомиться с положениями документа «Руководство администратора» и «Руководство пользователя», приведенные на веб-сайте https://auroraos.ru/documentation#!/tab/565511138-1.

ПРИМЕЧАНИЕ. Внешний вид интерфейса Аврора TEE может отличаться от приведенного на рисунках в настоящем документе. Снимки экрана являются примером и представлены для общего ознакомления.

СОДЕРЖАНИЕ

1. УСТАНОВКА АВРОРА TEE

Аврора TEE устанавливается на устройство вместе с ОС Аврора, если предусмотрено конфигурацией для Вашего устройства.

ПРИМЕЧАНИЕ. Выполнения дополнительных действий для установки не требуется.

2. РАБОТА С АВРОРА TEE

2.1. Первичная инициализация МУ

Рисунок 1

При первой загрузке мобильного устройства (МУ) пользователю необходимо сгенерировать аппаратный ключ защиты (Рисунок 1), который будет записан в однократно-программируемую память (efuse).

Для запуска процесса создания аппаратного ключа защиты выполнить следующие действия:

– несколько раз коснуться экрана МУ для начала заполнения индикатора загрузки (Рисунок 2);

– прекратить касаться экрана МУ после полного заполнения индикатора загрузки (Рисунок 3).

ВНИМАНИЕ! После генерации аппаратного ключа защиты сгенерировать новый будет невозможно.

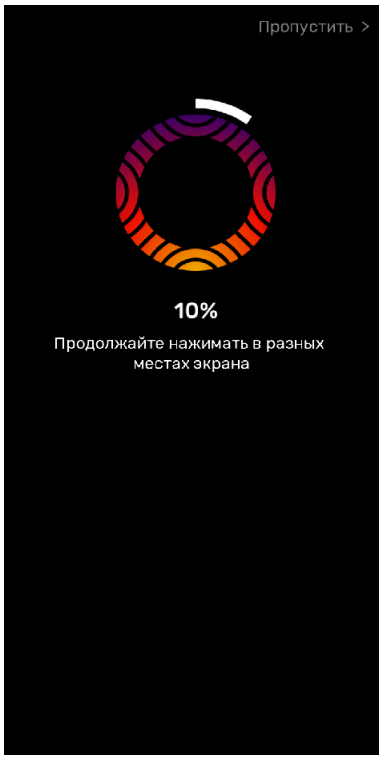

Рисунок 2

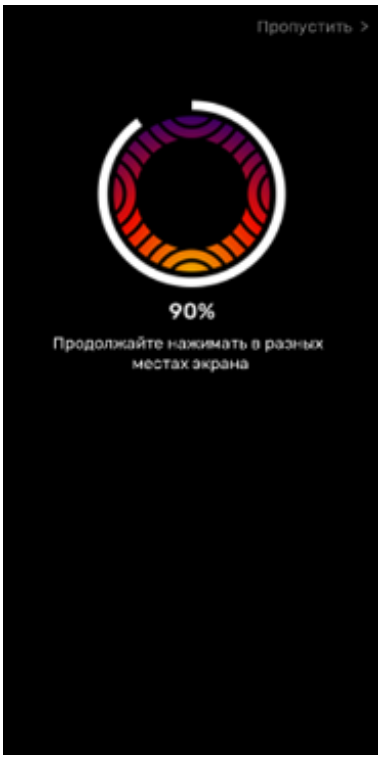

Рисунок 3

2.2. Пропуск создания аппаратного ключа защиты

Рисунок 4

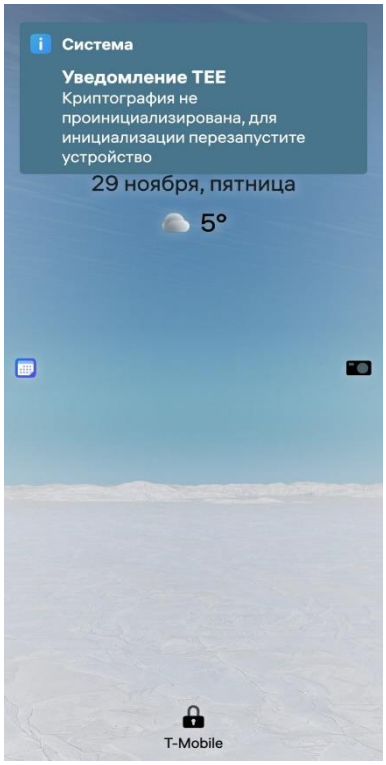

Рисунок 5

ВНИМАНИЕ! Криптография на основе Аврора TEE требует инициализации датчика случайных чисел (ДСЧ) при первом запуске устройства. В случае, если сбор данных для ДСЧ был пропущен, на Экране блокировки (Рисунок 5) и Экране событий будет показано уведомление об отключенной криптографии на основе Аврора TEE, а также могут наблюдаться проблемы в работе приложений, использующих криптографию.

ПРИМЕЧАНИЕ. Подробная информация об Экране блокировки и Экране событий приведено в документе «Руководство пользователя».

Для пропуска создания аппаратного ключа защиты необходимо выполнить следующие действия:

– коснуться кнопки «Пропустить» (см. Рисунок 1);

– на открывшейся странице выполнить одно из следующих действий (см. Рисунок 4):

- в левом верхнем углу коснуться кнопки «Назад» либо кнопки «Продолжить загрузку» для возврата к процессу создания аппаратного ключа защиты;
- коснуться кнопки «Выключить устройство» для выключения МУ.

ВНИМАНИЕ! В случае пропуска создания аппаратного ключа защиты при последующей загрузке МУ отобразится соответствующее уведомление (Рисунок 5).

2.3. Аутентификация при повторных включениях

При повторных включениях во время загрузки МУ отображаются экраны, представленные на рисунках (Рисунок 6, Рисунок 7).

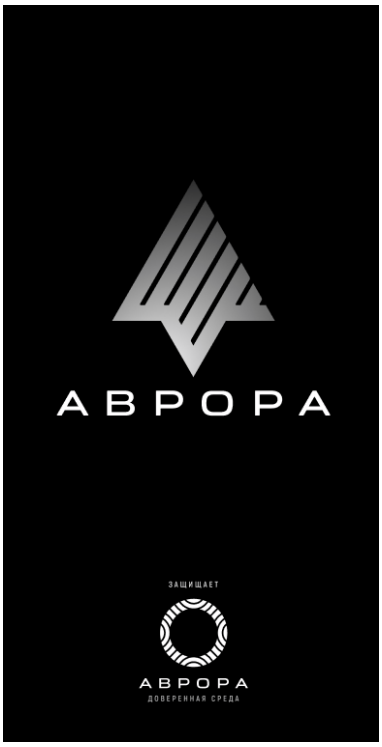

Рисунок 6

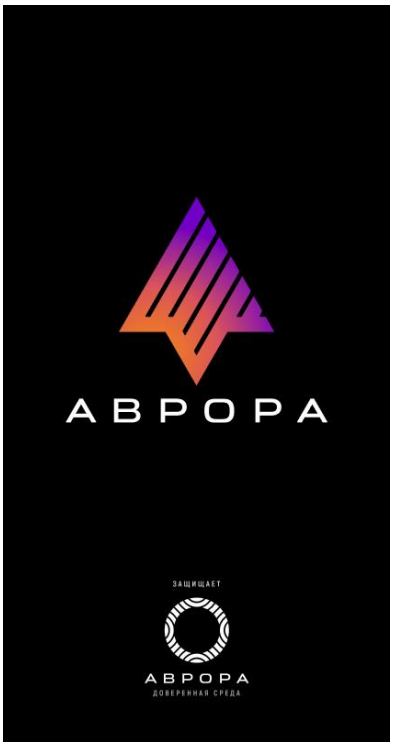

Рисунок 7

2.4. Возможные компроментации

2.4.1. Компрометация МУ

Рисунок 8

Компрометацией МУ является обнаружение нарушения целостности кода программного обеспечения или статических данных ОС Аврора. В случае компрометации МУ на экране отобразится соответствующее сообщение (Рисунок 8).

Для продолжения работы МУ необходимо коснуться кнопки «Продолжить работу».

ПРИМЕЧАНИЕ. Возможность продолжения работы становится доступной по истечении 10 секунд после появления сообщения о компрометации МУ (Рисунок 8).

– Для выключения МУ необходимо коснуться кнопки «Выключить устройство» (Рисунок 8).

2.4.2. Компрометация аппаратного ключа защиты

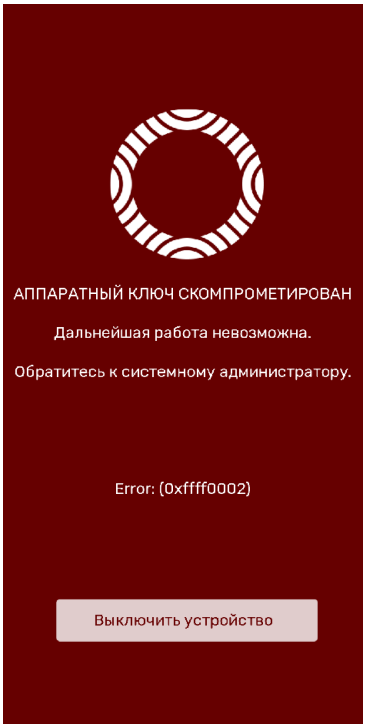

Рисунок 9

В случае компрометации аппаратного ключа защиты на экране МУ отобразится сообщение с описанием причины и указанием кода ошибки (Рисунок 9).

Для выключения МУ необходимо коснуться кнопки «Выключить устройство» (Рисунок 9).

2.5. Возможные ошибки

2.5.1. Ошибка инициализации аппаратного ключа защиты

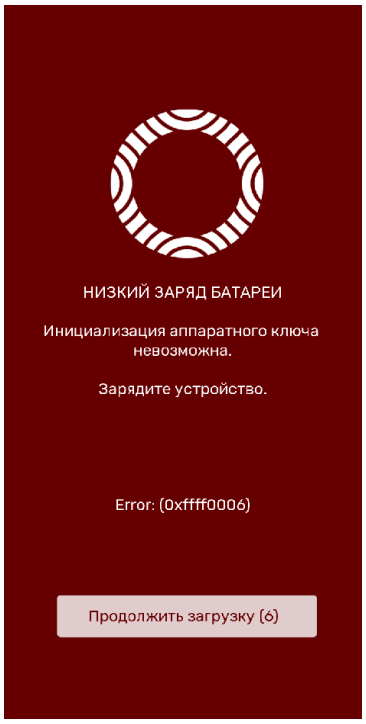

Рисунок 10

При низком заряде аккумулятора (менее 60%) может возникнуть ошибка инициализации аппаратного ключа защиты и на экране МУ отобразится сообщение с описанием причины и указанием кода ошибки (Рисунок 10).

Для продолжения загрузки МУ необходимо выполнить одно из следующих действий:

– коснуться кнопки «Продолжить загрузку»;

– дождаться автоматической загрузки по истечении 6 секунд (Рисунок 10).

2.5.2. Ошибка повторной инициализации аппаратного ключа защиты

Рисунок 11

При повторной инициализации аппаратного ключа защиты может возникнуть ошибка и на экране МУ отобразится сообщение с описанием причины (Рисунок 11).

Для продолжения загрузки МУ необходимо коснуться кнопки «Продолжить загрузку» (Рисунок 11).

Для выключения МУ необходимо коснуться кнопки «Выключить устройство» (Рисунок 11).

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 1).

Таблица 1

Термин/ Сокращение	Расшифровка
Аврора TEE	Доверенная среда исполнения Аврора
ДСЧ	Датчик случайных чисел
МУ	Мобильное устройство
ОС	Операционная система

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Содержание изменения	ФИО	Дата
1.0	Начальная версия	Аносов С.	26.06.2025 г.