

ИНСТРУКЦИЯ ПО ПРОВЕРКЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Листов 6

АННОТАЦИЯ

Настоящий документ является инструкцией по проверке электронной подписи (ЭП) загрузочного модуля Прикладного программного обеспечения «Аврора Центр» (далее – ППО).

ППО является прикладным программным обеспечением со встроенными механизмами защиты информации от несанкционированного доступа, предназначенным для:

- управления устройствами ¹, функционирующими под управлением операционной системы (ОС) Аврора, ОС Android и ОС семейства Linux;
- управления жизненным циклом приложений²;
- отправки push-уведомлений на устройства (кроме устройств под управлением ОС семейства Linux);

– обновления ОС Аврора и ОС семейства Linux путем получения из доверенного хранилища пакетов с изменениями ОС (образа ОС) и их установки. При этом указанные процессы выполняются штатными средствами самой ОС, а ППО участвует лишь в их инициализации в ОС и не гарантирует их успешного завершения;

- автоматизированной обработки следующих видов информации:
 - общедоступной информации;
 - информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, подлежащей защите в соответствии с требованиями действующего законодательства Российской Федерации в области информационной безопасности.

¹ Определение термина «Устройство» приведено в таблице (Таблица 2).

² Определение термина «Приложение» приведено в таблице (Таблица 2).

СОДЕРЖАНИЕ

1. Проверка электронной подписи загрузочного модуля	4
Перечень терминов и сокращений.....	6

1. ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ ЗАГРУЗОЧНОГО МОДУЛЯ

Проверка ЭП загрузочного модуля осуществляется в ОС семейства Linux с помощью скрипта `verify-sign.sh`.

Для проверки ЭП необходимо выполнить следующие действия:

- 1) Получить у Разработчика ППО:
 - сертификат ключа проверки ЭП;
 - скрипт проверки ЭП;
 - файл с ЭП.

ПРИМЕЧАНИЕ. Сертификат ключа проверки ЭП и скрипт проверки ЭП должны быть получены по доверенному каналу связи (например, лично в офисе предприятия-изготовителя, либо загружен с сайта предприятия-изготовителя, с использованием защищенного канала связи);

2) Назначить пользователю право на выполнение скрипта с помощью команды:

```
chmod +x verify-sign.sh
```

- 3) Выполнить проверку ЭП.

Для того, чтобы выполнить проверку ЭП необходимо выполнить следующую команду:

```
./verify-sign.sh --dir [каталог с дистрибутивом] --cert [сертификат  
ключа проверки ЭП] --sign [файл с ЭП]
```

Например, для проверки ЭП оптического диска, примонтированного к каталогу `/media/omp/CDROM/`, необходимо выполнить команду:

```
./verify-sign.sh --dir /media/omp/CDROM/ --cert cacert.pem --sign  
distr.sign
```

Параметры запуска скрипта приведены в таблице (Таблица 1).

Таблица 1

Параметр	Описание
-h, --help	Вывод справки
-d, --dir	Каталог с загрузочным модулем ППО
-c, --cert	Сертификат ключа проверки ЭП
-s, --sign	Файл с ЭП

ПРИМЕЧАНИЕ. В каталоге с загрузочным модулем ППО должны находиться следующие каталоги: `checksums`, `docs`, `mobile-apps`, `server`. Содержимое каталога с загрузочным модулем может отличаться в зависимости от версии ППО.

В случае успешной проверки будет выведено сообщение:

```
Verified OK
```

В случае не успешной проверки будет выведено сообщение:

```
Verification Failure
```

В данном случае, необходимо убедиться, что в загрузочный модуль не были внесены изменения, после чего обратиться в службу технической поддержки предприятия-изготовителя ППО, приложив следующие файлы:

- файл с контрольными суммами (путь к файлу: `~/verify_distr_sign/distr.md5`);
- файл с ЭП;
- сертификат открытого ключа проверки ЭП.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 2).

Таблица 2

Термин/ Сокращение	Расшифровка
ОС	Операционная система
ППО	Прикладное программное обеспечение «Аврора Центр»
Предприятие-разработчик, предприятие-изготовитель	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
Приложение	Приложением является: – мобильное приложение, функционирующее под управлением ОС Аврора/ОС Android; – приложение для ЭВМ, функционирующей под управлением ОС семейства Linux
Устройство	Под устройством подразумевается мобильное устройство и/или ЭВМ, на которой функционируют соответствующие компоненты ППО
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись