

Ключи Guardant в Linux и Wine

Данная инструкция предназначена для пользователей, использующих **Guardant SDK** для защиты приложений.

Работают ли ключи Guardant под Linux

Да, работают. Нативная поддержка GNU/Linux реализована в моделях [Guardant Sign](#) / [Time](#) / [Code](#), а так же в их [сетевых версиях](#).

Предыдущие модели электронных ключей Guardant (Guardant Stealth III / Net III / Stealth II USB / Net II USB) не могут работать под Linux «самостоятельно». Максимум, что можно сделать в этом случае — запускать Windows-приложение, защищенное с помощью этих ключей, в среде коммерческой сборки [WINE@Etersoft](#).

Что нужно для работы

Для ключей Guardant, которые поддерживают Linux, не требуется никакого специального драйвера. В системе нужно просто установить специальное правило (архив [udev-rules.tar.gz](#) в папке с установленным SDK `..\Guardant\SDK7\Redistribute\Linux\`). Подробная инструкция есть в соответствующем [разделе](#) портала документации.

Работают ли ключи Guardant в среде Wine

Да, работают. Полная поддержка Wine реализована в моделях [Guardant Sign](#) / [Time](#) / [Code](#).

Обратите внимание!

Работа предыдущих моделей электронных ключей Guardant (Guardant Stealth III / Net III / Stealth II USB / Net II USB) возможна только в среде коммерческой сборки [WINE@Etersoft](#).

Что нужно для работы

Для работы Windows-приложений, защищенных ключами [Sign](#) / [Time](#) / [Code](#) в среде Wine, необходимо наличие в системе библиотеки **grdwine.dll.so**. Эта библиотека поставляется в виде исходных кодов. Подробная инструкция по компиляции и работе с библиотекой есть в соответствующем [разделе](#) портала документации.

Более того, в некоторые дистрибутивы Linux (например, [ALTLinux](#)) включена открытая сборка WINE@Etersoft, уже содержащая **grdwine.dll.so**. В случае использования такого дистрибутива никаких дополнительных действий, кроме установки правил для работы с ключами, не требуется (тесты выполнялись на WINE from Etersoft public 1.1.18).

Как защитить приложение под Linux

Защита Linux-приложений основана на использовании [Guardant API](#). Приложение с интегрированными функциями Guardant API компилируется в среде GNU/Linux со специальной библиотекой, входящей в состав комплекта разработчика. Подробная инструкция по компиляции и работе с библиотекой содержится в соответствующем [разделе](#) портала документации.

Напоминаем, что GNU/Linux поддерживают только ключи [Guardant Sign](#) / [Time](#) / [Code](#).

Приложение не видит ключ под Linux, хотя все необходимые правила созданы

Эта ситуация может быть вызвана системой принудительного [контроля доступа SELinux](#). Если SELinux используется с настройками по умолчанию в режиме «принудительный» или «предупреждающий», то электронные ключи не будут доступны.

Наиболее характерно такое положение для дистрибутивов, в которых SELinux предлагается установить непосредственно при установке системы (к примеру Fedora, CentOS, и другие).

Чтобы решить проблему, достаточно изменить контекст безопасности для защищенного приложения:

```
# chcon -t textrel_shlib_t '/home/usr/test'
```

После этого файл с именем «test», расположенный в каталоге `/home/usr` сможет работать с электронным ключом [Guardant Sign](#) / [Time](#) / [Code](#)