Поддержка ЭЦП в ОС из Реестра отечественного ПО

Дмитрий Державин
Базальт СПО, ведущий инженер

Краткое резюме

- в целом — всё работает
- есть нюансы
- подробности: https://www.altlinux.org/ЭЦП

Постановка задачи

- ПП № 1236 (запрет на допуск иностранного ПО), 188-ФЗ (запрет на закупку для госорганов ПО, не входящего в Реестр), Распоряжение № 1588-р и т. д.
- Реестр отечественного ПО
- поддержка ГОСТ
- Госуслуги, Госзакупки, ЭТП и т. д. и т. п.
- подпись файлов

Условия тестирования

- используем ОС Альт
- действуем на общих основаниях
- выполняем проверки не на модельных, а на реальных задачах
- обеспечиваем по возможности максимальный уровень защищённости (пытаемся избежать расширения модели угроз)

Текущий уровень поддержки

- поддержка современных устройств на уровне протоколов PC/SC и CCID
- поддержка произвольных библиотек PKCS#11 на уровне реализованных в них возможностей
- поддержка алгоритмов ГОСТ на уровне подписи документов
- поддержка алгоритмов ГОСТ на уровне шифрования каналов передачи данных
- поддержка популярных программных криптопровайдеров

Выявленные проблемы

- носители данных ЭЦП, выдаваемые разными УЦ на общих основаниях, могут быть несовместимы между собой
- носители данных ЭЦП, выдаваемые разными УЦ на общих основаниях, могут быть несовместимы с порталами государственных услуг и сайтами ЭТП

Выявленные неожиданности

- уровень защищённости носителей данных ЭЦП, массово выдаваемых конечным пользователям, как правило, существенно занижен
- разработчики порталов государственных услуг и сайтов ЭТП могут рекомендовать пользователям заведомо небезопасные программно-аппаратные конфигурации

Потенциальные проблемы

- прекращение поддержки NPAPI в браузерах
- прекращение поддержки ГОСТ Р 34.10-2001
- неготовность УЦ работать с запросами на подпись

Спасибо за внимание!

Дмитрий Державин <dd@basealt.ru>