

ПРОТОКОЛ № 8223/2022

проведения совместных испытаний USB-токена JaCarta PKI JC200 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6)

г. Москва

20 июля 2022 г.

1 Предмет испытаний

1.1 В настоящем Протоколе зафиксировано, что в период с 31.05.2022г. по 20.07.2022г. были проведены совместные испытания USB-токена JaCarta PKI JC200 (далее — Устройство) с операционной системой специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) (далее — ОС Astra Linux 1.6), разработанной ООО «РусБИТех-Астра», включая ОС Astra Linux 1.6 с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 20211126SE16 (далее — ОС Astra Linux 1.6.10).

2 Объект испытаний

2.1 На испытания был предоставлено Устройство в следующей комплектации: USB-токен, ПО для него (установлено приложение «PKI») и сопроводительная документация.

3 Ход испытаний

3.1 В ходе совместных испытаний была проведена проверка корректности определения и функционирования устройства в ОС Astra Linux 1.6 и ОС Astra Linux 1.6.10 в объеме проверок, указанных в Приложении 1. Проверки осуществлялись с использованием эксплуатационной документации на ОС Astra Linux 1.6.

3.2 Ход испытаний описан в Приложении 2.

3.3 Для проверки работоспособности следующих узлов было дополнительно установлено ПО:

Устройство	Наименование ПО	MD5	Источник ПО
USB-токен	ПК «Единый Клиент JaCarta» jacartauc_2.13.10.3184_al1.6_x64.zip	76490b4b088c135188466 e63009e8b5d	Скопировано с сайта АО «Аладдин Р.Д.»
	«КриптоПро CSP 5.0.12500» linux-amd64_deb.tgz	9ba29d15fad621038257 0e85a9f5749	Скопировано с сайта ООО «КРИПТО-ПРО»
	cproccsp-rdr-jacarta-64_5.0.12500- 6_amd64.deb	fc31ae673b0be9481802fa 39955deddc	Скопировано с сайта ООО «КРИПТО-ПРО», входит в архив linux-amd64_deb.tgz

4 Результаты испытаний

4.1 По результатам тестирования установлено, что Устройство под управлением ОС Astra Linux 1.6 и ОС Astra Linux 1.6.10 функционирует **КОРРЕКТНО**.



Вывод

Устройство с установленной ОС Astra Linux 1.6 и ОС Astra Linux 1.6.10 пригодно к применению с учетом п.1.7 Приложения 2

5 Состав рабочей группы и подписи сторон

Настоящий Протокол составлен рабочей группой:

Кулик А. Ю. – руководитель сектора испытаний на совместимость с СВТ отдела тестирования на совместимость департамента развития технологического сотрудничества ДВИС ООО «РусБИТех-Астра»;

Лукина Е. В. – старший инженер отдела тестирования на совместимость департамента развития технологического сотрудничества ДВИС ООО «РусБИТех-Астра».

ООО «РусБИТех-Астра»

руководитель сектора испытаний на совместимость с СВТ
отдела тестирования на совместимость департамента
развития технологического сотрудничества ДВИС

(должность)

Кулик А. Ю.

(подпись)

(фамилия, инициалы)

« ____ » _____ 20 ____ года



Перечень функциональных проверок Устройства

Наименование проверки		Результат испытаний	
Версия операционной системы		1.6.0	1.6.10
1.	Обнаружение токена в ОС	Успешно	Успешно
2.	Создать криптоконтейнер (использовались самозаверенные сертификаты сгенерированные в ХСА)	Успешно	Успешно
3.	Проверка работы контейнера:		
3.1	Просмотр содержимого	Успешно	Успешно
3.2	Размещение тестового сертификата открытого ключа	Успешно	Успешно
3.3	Установка, экспорт, удаление сертификата	Успешно	Успешно
3.4	Подписание документа электронной присоединённой подписью	Успешно	Успешно
3.5	Удаление контейнера	Успешно	Успешно
3.6	Шифрование/расшифрование файла	Успешно	Успешно
3.7	ЭП для web-сервисов (демо-портал «КриптоПро»)	Успешно	Успешно
4.	Проверка двухфакторной аутентификации, локально	Успешно	Успешно



Описание хода проведения испытаний

1 Ход испытаний

1.1 В ходе совместных испытаний установлено, что в среде Astra Linux 1.6 необходимо доустановить пакеты libpcre16-3, pcscd и pcsc-tools с диска с оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 20211126SE16.

1.2 Для определения устройства в системе использовалась утилита pcsc-tools консольная команда:

```
pcsc_scan
```

1.3 Необходимо установить пакет cprosp-rdr-jakarta-64_5.0.12500-6_amd64.deb из состава «КриптоПро CSP 5.0.12500» чтобы данное ПО могло взаимодействовать с токеном.

1.4 В ходе совместных испытаний установлено, что при использовании графического приложения «Цифровые сертификаты ХСА», приложение USB-токена с интегрированным приложением «PKI», позволяет производить экспорт как сертификата, так и ключа, с тем условием что при генерации ключа в качестве его хранилища указывается токен. Создание криптоконтейнера производилось при помощи установленного в ОС приложения «Цифровые сертификаты ХСА» и сгенерированных им самозаверенных сертификатов.

1.5 Для проверки локальной двухфакторной аутентификации использовалась тестовая версия ПО «SecurLogon», предоставленная производителем. Так как эта версия ещё будет дорабатываться, в данном протоколе не указана версия ПО и его md5 хэш.

1.6 Проверки функционала производились в ядрах ОС Astra Linux 1.6: 4.15.3-1 «generic» и «hardened» и ОС Astra Linux 1.6.10: 4.15.3-154, 5.4.0-81, 5.10.0-1045 «generic» и «hardened» соответственно.

1.7 Работоспособность электронной подписи (далее - ЭП) для web-сервисов проверялась с помощью демо-портала «КриптоПро» ЭЦП браузер плагин https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html и ПО «КриптоПро CSP 5.0.12500» установленного в среде ОС. Демо-портал «Аладдин Р.Д.» <https://demo.aladdin-rd.ru/> не взаимодействует с приложением «PKI», для сохранения сертификата на данном ресурсе используется только приложение «ГОСТ».

1.8 Проверка работы контейнера (просмотр содержимого, генерация, установка, экспорт, удаление сертификата и прочее) производилась с помощью ПО «КриптоПро CSP 5.0.12500» и сертификатов сгенерированных на демо-портале «КриптоПро» <https://testca.cryptopro.ru/certsrv/>.



Приложение № 3 к Протоколу № 8223/2022

Перечень используемых сокращений

ОС Astra Linux 1.6 — операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6);

ОС Astra Linux 1.6.10 — ОС Astra Linux 1.6 с установленным оперативным обновлением БЮЛЛЕТЕНЬ № 20211126SE16;

ОС — операционная система;

Устройство — USB-токен JaCarta PKI JC200;

Токен — устройство с защищенной паролем картой памяти, на которой хранится информация для создания подписи, может быть в виде USB-накопителя либо смарт-карты;

ЭП — электронная подпись позволяет подтвердить авторство электронного документа, это его реквизит полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи.

Идентификатор документа 6b2fed8a-0e18-4da8-af40-40878b8fff4b

Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

Подписи отправителя:	Владелец сертификата: организация, сотрудник	Сертификат: серийный номер, период действия	Дата и время подписания
 ООО "РУСБИТЕХ-АСТРА" Кулик Александр Юрьевич, Руководитель группы по тестированию на совместимость с СВТ	020C70AE0046AE97BB494C124B4E6E35CF с 24.02.2022 13:25 по 24.02.2023 13:35 GMT+03:00	26.07.2022 13:59 GMT+03:00 Подпись соответствует файлу документа	