

ПРОТОКОЛ № 8225/2022

проведения совместных испытаний USB-токена JaCarta PKI JC200 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва

30 июня 2022 г.

1. Предмет испытаний

1.1 В настоящем Протоколе зафиксировано, что в период с 31.05.2022г. по 30.06.2022г. 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 1.7) (далее — ОС Astra Linux 1.7), разработанной ООО «РусБИТех-Астра», включая ОС Astra Linux 1.7 с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2021-1126SE17 (далее — ОС Astra Linux 1.7.1).

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 1.7 и ОС Astra Linux 1.7.1 в объеме проверок, указанных в Приложении 1 и Приложении 2. Проверки осуществлялись с использованием эксплуатационной документации на ОС Astra Linux 1.7.

3.2 Ход испытаний описан в Приложении 3.

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.»
	«JC-WebClient» JCWebClient_4.3.2.1520_Linux_DEB _x64.deb	3520dc153d2844849f725 501c2a44b9f	Скопировано с сайта АО «Аладдин Р.Д.»
	«КриптоПро CSP 5.0.12500» linux-amd64_deb.tgz	9ba29d15fad621038257 0e85a9f5749	Скопировано с сайта ООО «КРИПТО-ПРО»



4 Результаты испытаний

4.1 По результатам тестирования установлено, что Устройство под управлением ОС Astra Linux 1.7 и ОС Astra Linux 1.7.1 функционирует **КОРРЕКТНО**.

Вывод

Устройство с установленной ОС Astra Linux 1.7 и ОС Astra Linux 1.7.1 пригодно к применению.

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



Приложение № 1 к Протоколу № 8225/2022

Перечень функциональных проверок Устройства

Наименование проверки		Результат испытаний	
Версия операционной системы		1.7.0	
Версия ядра Astra Linux		5.4.0-54-generic	5.4.0-54-hardened
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 подписью присоединённой	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



Перечень функциональных проверок Устройства

Наименование проверки		Результат испытаний	
Версия операционной системы		1.7.1	
Версия ядра Astra Linux		5.4.0-81-generic/hardened	5.10.0-1045-generic/hardened
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



Приложение № 3 к Протоколу № 8225/2022
Описание хода проведения испытаний

1 Ход испытаний

1.1 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.

1.2 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.

1.3 Для определения устройства в системе использовалась утилита pcsc-tools, она входит в состав дистрибутивного диска, использовалась консольная команда:

```
pcsc_scan
```

1.4 Создание криптоконтейнера производилось при помощи установленного в ОС приложения «Цифровые сертификаты ХСА» и сгенерированных им самозаверенных сертификатов.

1.5 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. Использовать для проверки этой функции демо-портал «Аладдин Р.Д.» <https://demo.aladdin-rd.ru/> не представлялось возможным, так как приложение «PKI» для сохранения сертификата на данном ресурсе не предусмотрено, только приложение «ГОСТ»

1.6 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 № 4 к Протоколу № 8225/2022

Перечень используемых сокращений

ОС Astra Linux 1.7 — операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7);

ОС Astra Linux 1.7.1 — ОС Astra Linux 1.7 с установленным оперативным обновлением БЮЛЛЕТЕНЬ № 2021-1126SE17;

ОС — операционная система;


Устройство — USB-токен JaCarta PKI JC200 с установленным приложением «PKI»;

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 6427d9f4-d4c4-4536-b8a9-a2140872a97c

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	020С70АЕ0046АЕ97ВВ494С124В4Е6Е35СF с 24.02.2022 13:25 по 24.02.2023 13:35 GMT+03:00	29.07.2022 10:11 GMT+03:00 Подпись соответствует файлу документа	

