ПРОТОКОЛ № 27686/2025

проведения совместных испытаний программного обеспечения "Центр Сертификации на основе криптографии OpenSSL (MiniCA)" версии 1.8.2 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8)

г. Москва 14.03.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 13.03.2025 по 14.03.2025 совместных испытаний программного обеспечения "Центр Сертификации на основе криптографии OpenSSL (MiniCA)" версии 1.8.2 (далее – ПО), разработанного ООО "Клируэй Текнолоджис", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) (далее – Astra Linux SE 1.8), разработанной ООО "РусБИТех-Астра".

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся в ходе проведения данных испытаний, относящихся к ПО, представлен в Таблице 1.

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	Наименование	MD5	Источник
Файл программного пакета дистрибутива ПО	minica-1.8.2-fd32ac3_amd64-2024.11.27-signed.run	D691D9E855B61F0F719C9B38E0DDA2A8	Сторона разработчика ПО
Файл программного пакета дистрибутива "СУБД Tantor SE"	tantor-se-server-16_16.2.1_amd64.deb	CABE305FBA34E548B12DA6908A9F1422	Сторона разработчика ПО
Официальное руководство по эксплуатации ПО в электронном формате	Электронная документация на ПО "Центр Сертификации на основе криптографии OpenSSL (MiniCA)"	–	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в среде Astra Linux SE 1.8, в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 С целью проведения проверок при включённом режиме ЗПС использовался файл открытого ключа разработчика ПО.

3.4 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.8.

5 Вывод

5.1 ПО и операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4 и Приложении 2.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Дмитриев В. Ю. – Архитектор отдела инфраструктуры, ООО "Клируэй Текнолоджис".

ООО "Клируэй Текнолоджис"

Архитектор отдела инфраструктуры

(должность)

Дмитриев В. Ю.

(подпись) (фамилия, инициалы)

Приложение 1 к Протоколу № 27686/2025

Перечень проверок совместимости ПО и Astra Linux SE 1.8

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE 1.8 с ядром ОС	
		6.1.90-1-generic	6.6.28-1-generic
1.	Установка ПО	Успешно	Успешно
2.	Эксплуатация ПО	Успешно	Успешно
3.	Удаление ПО	Успешно	Успешно
4.	Требования безопасности ALSE	Успешно	Успешно
5.	Механизм безопасности ЗПС	Успешно	Успешно
6.	Механизм безопасности МКЦ	Успешно	Успешно
7.	Механизм безопасности МРД	Не проводилась	Не проводилась

Приложение 2 к Протоколу № 27686/2025

Инструкция по установке и удалению ПО в среде Astra Linux SE 1.8

1 Используемые репозитории в Astra Linux SE 1.8:

- deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/main-repository/ 1.8_x86-64 main contrib non-free non-free-firmware

2 Установка ПО:

2.1 выполнить системные команды, действия:

2.1.1 ПО поставляется в виде саморазворачивающегося архива. Для установки выполнить файл или разархивировать его в любой каталог.

2.1.2 Отредактировать файл `preinstall.env`. Задать идентификатор ТУЗ от имени которой будет выполняться микросервис (`USER_NAME`), задать каталог для установки (`USER_PATH`).

2.1.3 Выполнить сценарий `preinstall.sh` от имени суперпользователя.

2.1.4 sudo ./preinstall.sh

2.1.5 Сценарий создаст технологическую учетную запись (по умолчанию minica) и каталог для установки микросервиса с необходимыми правами доступа.

2.1.6 Задать пароль для технологической учетной записи.

2.1.7 Скопировать файлы и каталоги дистрибутива в любой каталог, доступный для технологической учетной записи.

2.1.8 Выполнить вход или подключение через ssh по именем технологической учетной записи.

2.1.9 Отредактировать файл конфигурации `database.env`. Необходимо указать пароль для доступа к БД.

2.1.10 Создать базу данных PostgreSQL. Для создания БД воспользоваться вспомогательными сценариями `db-XX-*.sh` в каталоге `deploy`. Доступа к БД можно указать заранее в файле `conf/minica.yml` или после установки в файле `/app/itc/minica/conf/minica.yml` (если значение `USER_PATH` задано как "/app/itc/minica"). Также в этом файле необходимо определить значение `database -> url`.

2.1.11 Отредактировать файл `install.env` (при необходимости).

2.1.12 Отредактировать файл `config-ca.env`. Необходимо задать требуемые реквизиты для сертификата УЦ.

2.1.13 Отредактировать файл `config-tls.env`. Необходимо задать требуемые реквизиты для TLS сертификата.

2.1.14 Выполнить сценарий `install.sh`. Сценарий необходимо выполнять от имени технологической учетной записи, от имени которого будет выполняться микросервис. Данный сценарий выполнит скрипт `make-ca-cert.sh`, который создаст ключевую пару (`ca/ca.key`) и самоподписанный сертификат корневого ЦС (`ca/ca.crt`) и CSR запрос (ca/ca.csr), на основе которого может быть выпущен сертификата дочернего ЦС с использованием вышестоящего (обычно корневого ЦС).

Кроме того скрипт `make-tls-cert.sh` формирует ключевую пару (`ca/tls.key`) и первичный TLS сертификат (ca/tls.crt). В дальнейшем данный TLS сертификат и ключевая могут быть обновлены. CSR запрос сохраняется в файле (`ca/tls.csr`).

Примечание: В некоторых случаях потребуется изменить права доступа к файлам дистрибутива для доступа к ним со стороны заданной технологической учетной записи.

2.1.15 Опционально. Обновление ключа подписи запросов.

В составе дистрибутива поставляется демонстрационный ключ:

- `conf/itc.key` - ключевая пара/закрытый RSA ключ.
- `conf/itc.crt` - X.509v3 сертификат/контейнер открытого RSA ключа.

Путь к файлу `conf/itc.crt` указан в конфигурационном файле `conf/minica.yml`, а данный файл используется, если включена проверка подписи (опция `nosign` задака на `false`).

Закрытый ключ `itc.key` должен быть доступен для клиента MiniCA (в частности для утилиты mclient). Путь к файлу `conf/itc.key` указан в конфигурационном файле `conf/mclient.yml`.

Для обеспечения безопасности рекомендуется (для продуктовой среды требуется!) обновить данные ключи. Для обновления во время установки (до запуска `install.sh`) может использоваться сценарий `make-itc-key.sh`.

3 Удаление ПО:

3.1 выполнить действие:

Выполнить скрипт uninstall.sh. Сценарий необходимо выполнять от имени технологической учетной записи.

Приложение 3 к Протоколу № 27686/2025

Перечень используемых сокращений

Astra Linux SE 1.8 – операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8);

ЗПС – замкнутая программная среда;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение "Центр Сертификации на основе криптографии OpenSSL (MiniCA)" версии 1.8.2.