

ПРОТОКОЛ № 26347/2024

проведения совместных испытаний программного обеспечения "Центр Сертификации на основе криптографии OpenSSL (mini CA)" версии 1.8.2 и программного изделия СУБД "Tantor SE" версии 16.2.1

г. Москва

06.12.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 26.11.2024 по 05.12.2024 совместных испытаний программного обеспечения "Центр Сертификации на основе криптографии OpenSSL (mini CA)" версии 1.8.2, разработанного ООО "Клируэй Текнолоджис", и программного изделия СУБД "Tantor SE" версии 16.2.1, разработанного ООО "ТАНТОР ЛАБС".

2 Объект испытаний

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

Таблица 1 – Перечень пакетов дистрибутива

Описание	Наименование дистрибутива	MD5	Источник
Файл программного пакета дистрибутива "Центр Сертификации на основе криптографии OpenSSL (mini CA)"	minica-sfx-v1.8.2-fd32ac3_amd64-2024.11.27.run	3c9f0021a973163f6caa2013286909d9	Сторона разработчика ПО
Файл программного пакета дистрибутива СУБД "Tantor SE"	tantor-se-server-16_16.2.1_amd64.deb	CABE305FBA34E548B12DA6908A9F1422	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности совместного функционирования СУБД "Tantor SE" и "Центр Сертификации на основе криптографии OpenSSL (mini CA)" в объеме, указанном в Приложении 1.

3.2 В ходе испытаний использовался тестовый стенд описанный в Приложении 3.

4 Результаты испытаний

4.1 "Центр Сертификации на основе криптографии OpenSSL (mini CA)" корректно функционирует совместно с СУБД "Tantor SE".

5 Вывод

5.1 "Центр Сертификации на основе криптографии OpenSSL (mini CA)" версии 1.8.2 и СУБД "Tantor SE" версии 16.2.1 совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Гриньков А. В. – Архитектор отдела разработки ООО "Клируэй технолоджис";

Дмитриев В. Ю. – Ведущий архитектор отдела внедрения ООО "Клируэй технолоджис".

ООО "Клируэй Технолоджис"

Ведущий архитектор отдела внедрения

(должность)



(подпись)

Дмитриев В.Ю.

(фамилия, инициалы)

Приложение 1 к Протоколу № 26347/2024

**Перечень проверок совместимости "Центр Сертификации на основе
криптографии OpenSSL (mini CA)" и СУБД "Tantor SE"**

№ п/п	Наименование проверки	Результат проверки
1.	Инициализация соединения с СУБД "Tantor SE"	Успешно
2.	Функциональное тестирование	Успешно

Инструкция по интеграции "Центр Сертификации на основе криптографии OpenSSL (mini CA)" с СУБД "Tantor SE"

1 Настройка СУБД "Tantor SE".

Выполнить действия:

- 1.1 Установить ПО СУБД "Tantor SE" в соответствии с инструкцией производителя
- 1.2 Создать пользователя minica с правами администратора для доступа к СУБД.

2 Настройка "Центр Сертификации на основе криптографии OpenSSL (mini CA)".

Выполнить действия:

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

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

Выполнить сценарий ``preinstal.sh`` от имени суперпользователя

```
sudo ./preinstall.sh
```

Сценарий создаст технологическую учетную запись и каталог для установки микросервиса с необходимыми правами доступа

2.3 Отредактировать файл конфигурации ``databese.env``. Необходимо, как минимум, указать пароль для доступа к БД.

2.4 Создать базу данных PostgreSQL. Для создания БД воспользоваться вспомогательными сценариями ``db-XX-*.sh`` в каталоге ``deploy``.

2.5 Создать таблицы БД используя SQL схему ``deploy/sql/minica.up.sql``. URL 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``.

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

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

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

2.9 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.

2.10 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`.

Описание стенда

1. СУБД "Tantor SE" запущенный в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) на ядре 6.1.50-1 generic.

2. "Центр Сертификации на основе криптографии OpenSSL (mini CA)" запущенный в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) на ядре 6.1.50-1 generic

Перечень используемых сокращений

СУБД – система управления базами данных;

БД – база данных;

УЦ – удостоверяющий центр;

ЦС – центр сертификации;

ПО – программное обеспечение.