ТОО «НИЛ «Гамма Технологии»

Программное средство криптографической защиты информации «ТУМАР-CSP» версии 6.3

«Конфигуратор»

Инструкция по настройке профайла на устройство
398-600400083267- СКЗИ 17.2.12.1-6.3.3-2020

Алматы 2020

АННОТАЦИЯ

Настоящий документ является руководством пользователя по эксплуатации программного средства криптографической защиты информации «ТУМАР-CSP» версии 6.3 (далее по тексту – ПО «ТУМАР-CSP»), в частности, программного компонента «Tumar CSP. Конфигуратор» (далее по тексту – Конфигуратор).

В документе даны инструкции по созданию профайла для внешнего устройства хранения ключевой информации.

Документ предназначен для пользователей программы.

Все права на программное обеспечение ТУМАР-CSP принадлежат ТОО «НИЛ «Гамма Технологии» и не могут быть полностью или частично воспроизведены, тиражированы и распространены без разрешения Товарищества

ОГЛАВЛЕНИЕ

1 Терминология, сокращения и принятые обозначения

Носитель ключевой информации	устройство eToken PRO 72K, JaCarta, KAZTOKEN, SafeNet eToken 5110 – персональное средство строгой аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП
Профайл	набор настроек (Имя контейнера, Алгоритм ключей, Устройство хранения, параметр устройства хранения), сохраненный под определённым именем. Профайлы используются при загрузке и создании ключевой информации криптографическим модулем
Средство криптографической защиты информации	средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами
Удостоверяющий Центр	юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность сертификата
ОС	операционная система
ПО	программное обеспечение
СКЗИ	средство криптографической защиты информации
УЦ	Удостоверяющий Центр

Текст документации сопровождается различными элементами оформления в зависимости от его смыслового назначения. В таблице 1 приведены используемые условные обозначения.

Таблица 1 – Используемые условные обозначения

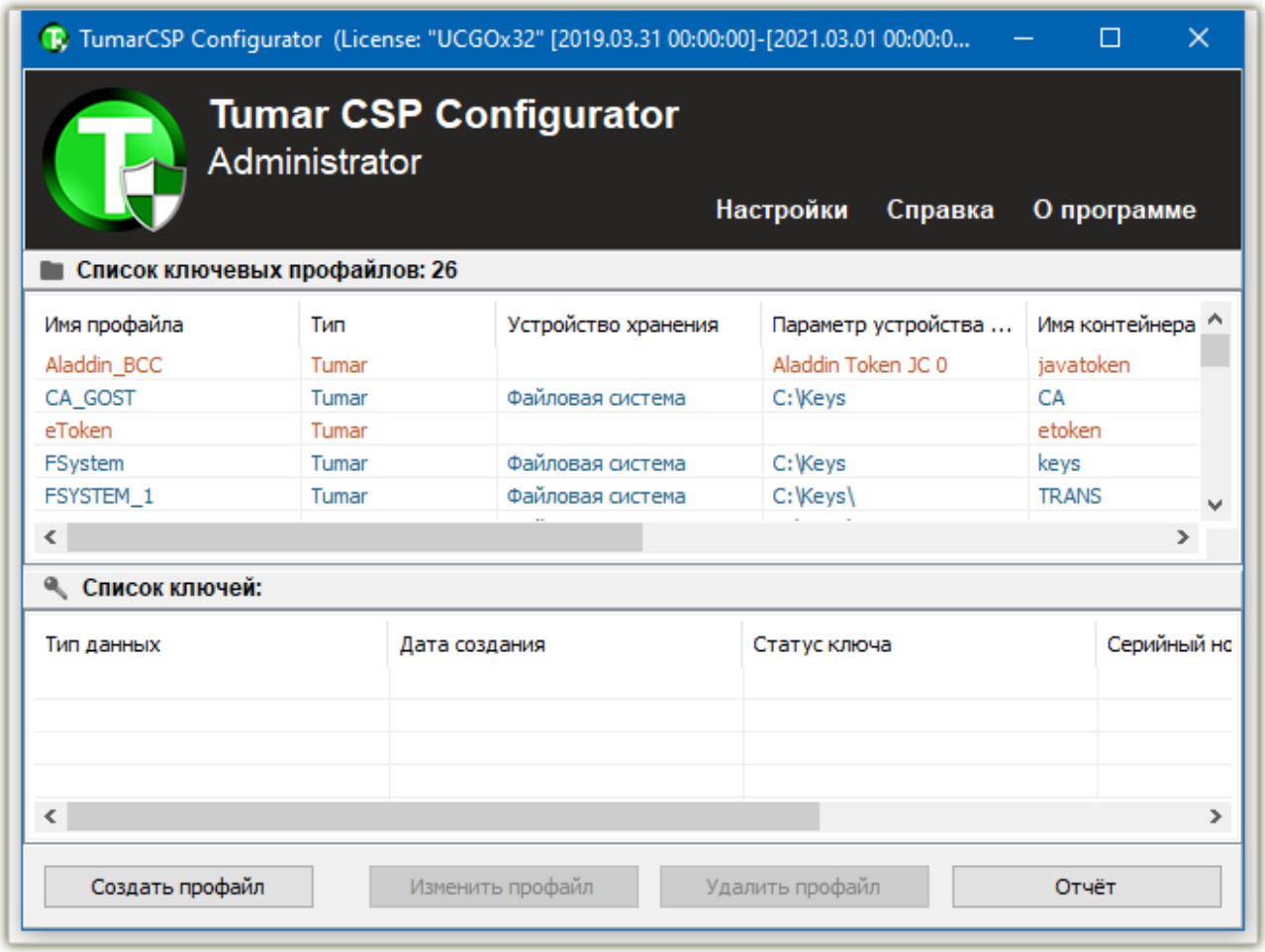
Условное обозначение	Назначение
	Важная информация, на которую следует обратить внимание
жирный шрифт	Названия меню, пунктов меню, окон, элементов управления
Курсив	Поля форм, предназначенные для заполнения
`текст информационных сообщений и командной строки`	Текст конфигурационных файлов, информационных сообщений программы и командной строки

2 Выполнение операций

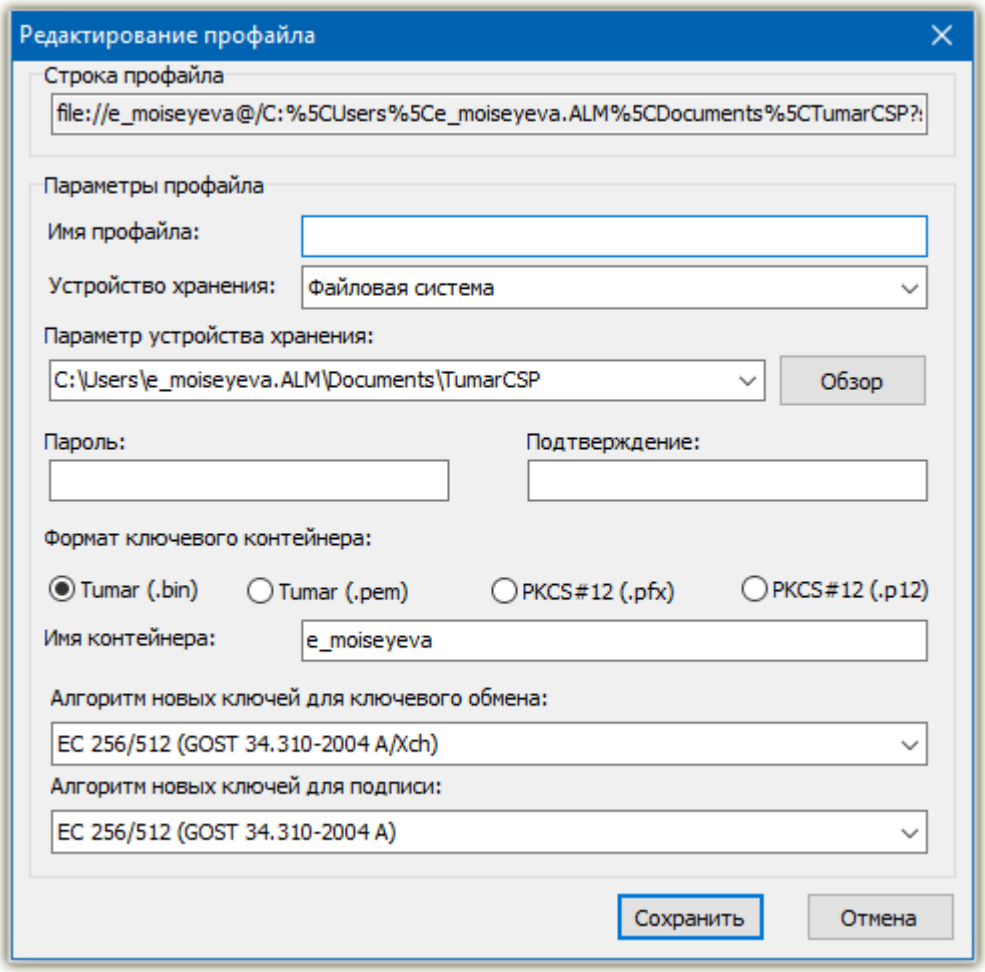
2.1 Создание профайла для внешнего устройства хранения

Для создания профайла следует выполнить следующие действия:

1. Подключить устройство к компьютеру.
2. Запустить Конфигуратор ПО «ТУМАР-CSP». На рабочем столе откроется главное окно программы в режиме администратора.



3. Нажать на кнопку **Создать профайл** для вызова диалогового окна настроек профайла.



4. В диалоговом окне **Редактирование профайла** заполнить следующие поля:

4.1. *Имя профайла* – ввести имя профайла, например, имя пользователя или наименование устройства, использующегося для выпуска ключей.

Параметр *Имя профайла* не должен содержать символов казахского языка. Поддерживаются латиница и кириллица. Допускается вводить в имя профайла следующие символы - 0-9, A-Z, «нижнее подчеркивание», «дефис».

4.2. *Устройство хранения* – выбрать из списка требуемое устройство хранения ключевого контейнера – *DigiFlow LLP & Aladdin Token JC& ARDS JaCarta* либо *New algorithm for tokens* (для работы с ГОСТ-kz алгоритмами) и т. д.

4.3. *Параметр устройства хранения* – установить значения, приведенные в Таблице 2, в соответствии с подключенным устройством:

Таблица 2. Взаимосвязь параметров настройки профайла от используемого устройства хранения ключевой информации.

Внешнее устройство	**Устройство хранения**	**Параметр устройства хранения*****
eToken PRO 72K	DigiFlow LLP. & Aladdin Token	Aladdin Token JC 0, Aladdin Token JC 1 и

Внешнее устройство	Устройство хранения	Параметр устройства хранения***
(Java)	JC & ARDS JaCarta	т.д. по порядку подключения устройств
	New algorithm for tokens*	Aladdin Token JC 0, Aladdin Token JC 1 и т.д. по порядку подключения устройств
JaCarta	DigiFlow LLP. & Aladdin Token JC & ARDS JaCarta	ARDS JaCarta 0, ARDS JaCarta 1 и т.д. по порядку подключения устройств
	New algorithm for tokens*	ARDS JaCarta 0, ARDS JaCarta 1 и т.д. по порядку подключения устройств
	jaCarta Laser**	asepkcs.dll
KAZTOKEN, версии 1.4	DigiFlow LLP. & Aladdin Token JC & ARDS JaCarta	DigiFlow LLP. KAZTOKEN 0, DigiFlow LLP. KAZTOKEN 1 и т.д. по порядку подключения устройств
SafeNet eToken 5110	DigiFlow LLP. & Aladdin Token JC & ARDS JaCarta	SafeNet Token JC 0, SafeNet Token JC 1 и т.д. по порядку подключения устройств
	New algorithm for tokens*	SafeNet Token JC 0, SafeNet Token JC 1 и т.д. по порядку подключения устройств

*Плагин для работы с ГОСТ-KZ алгоритмами

**Плагин необходим для работы с тонким клиентом WYSE (ключевая информация генерируется в Laser-аплет компании Аладдин Р.Д.). Для генерации ключей с использованием плагина требуется установка PKI Client. Плагин jaCarta Laser поддерживает только ключи алгоритма RSA (ниже 4096 бит)

***Если на компьютере пользователя установлено ПО «Safenet Authentication Client», то необходимо изменить «Параметр устройства хранения» во всех профайлах, в которых указано «Aladdin Token JC 0», на «AKS ifdh 0».

4.4. *Пароль* – ввести в поле пароль (PIN) для доступа к устройству хранения. Вводимый пароль отображается в полях в скрытом виде – (**********).

Используемый по умолчанию пароль:

- для eToken PRO 72K– 1234567890.
- для KAZTOKEN – 12345678.
- для JaCarta – 1234567890.
- SafeNet eToken 5110 – 1234567890.

4.5. *Подтверждение* – ввести в поле пароль (PIN) для доступа к ключевому контейнеру, аналогичный введенному паролю по п.4.4.

4.6. *Имя контейнера* – ввести наименование контейнера. По умолчанию именем контейнера является имя учетной записи пользователя в системе.

4.7. Выбрать *Алгоритм новых ключей для ключевого обмена* и *Алгоритм новых ключей для подписи* из выпадающего списка доступных алгоритмов формирования ключей. По умолчанию установлены следующие значения:

4.7.1 **В случае выпуска ключевой информации на алгоритмах ГОСТ**:

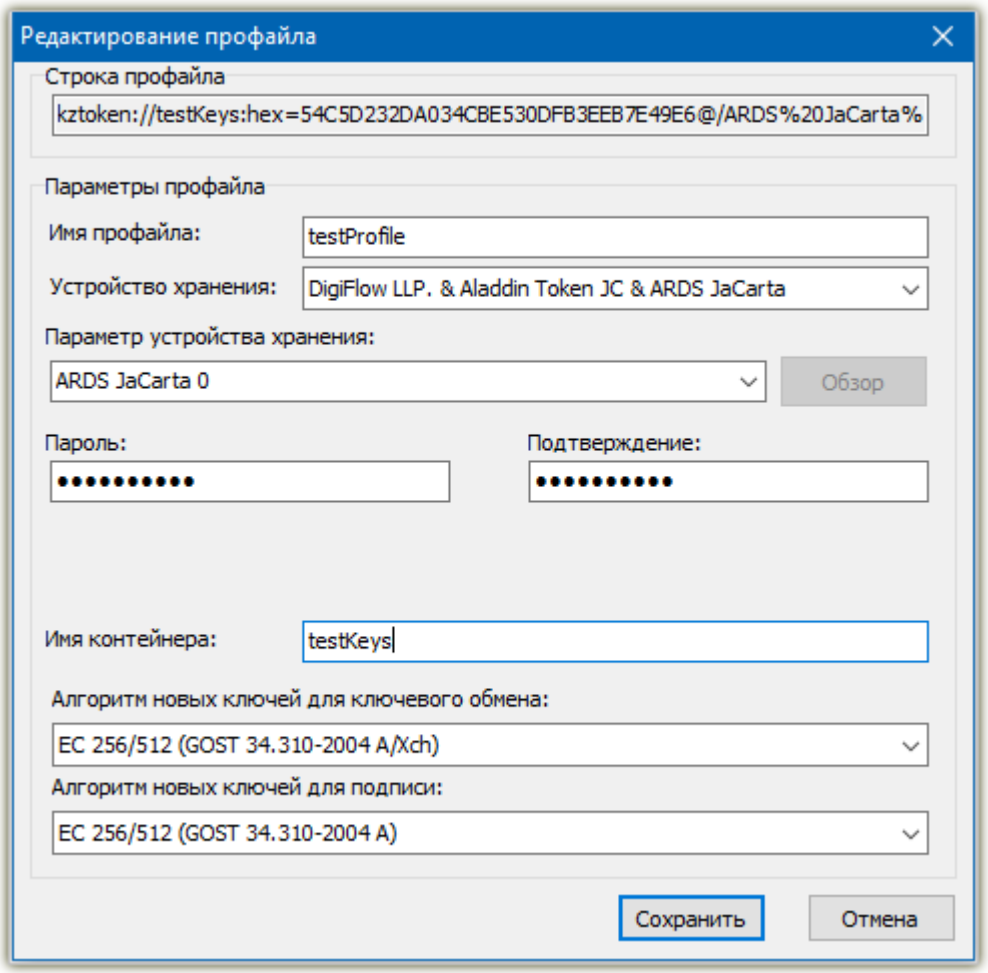
– Алгоритм новых ключей для ключевого обмена – EC 256/512(GOST 34.310-2004 A/Xch).

– Алгоритм новых ключей для подписи – EC 256/512(GOST 34.310-2004 A).

Генерация ключей алгоритма RSA на внешние носители невозможна, т.к. отсутствует

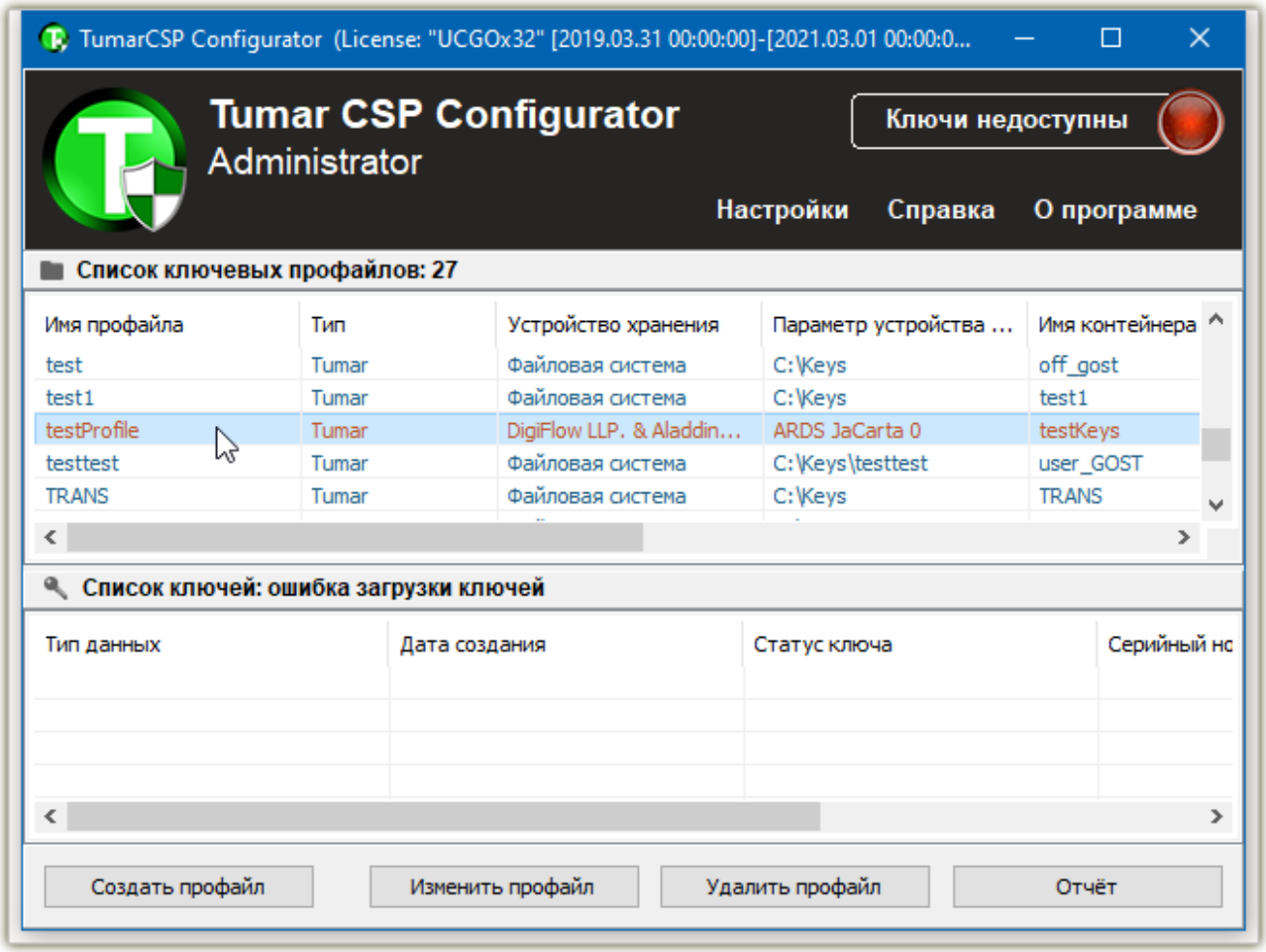
поддержка длины ключа RSA 4096.

4.8. После заполнения полей согласно пп.4.1-4.7 диалоговое окно **Редактирование профайла** для устройства выглядит следующим образом:



4.9. Нажать на кнопку **Сохранить**.

4.10. При корректном выполнении операции – отображение сформированного профайла для внешнего носителя в списке доступных профайлов.


TumarCSP Configurator (License: "UCGOx32" [2019.03.31 00:00:00]-[2021.03.01 00:00:0...
Tumar CSP Configurator
Administrator
Ключи недоступны
Настройки
Справка
О программе
Список ключевых профайлов: 27
Имя профайла
Тип
Устройство хранения
Параметр устройства ...
Имя контейнера
test
Tumar
Файловая система
C:\Keys
off_gost
test1
Tumar
Файловая система
C:\Keys
test1
testProfile
Tumar
DigiFlow LLP. & Aladdin...
ARDS JaCarta 0
testKeys
testtest
Tumar
Файловая система
C:\Keys\testtest
user_GOST
TRANS
Tumar
Файловая система
C:\Keys
TRANS
Список ключей: ошибка загрузки ключей
Тип данных
Дата создания
Статус ключа
Серийный нс
Создать профайл
Изменить профайл
Удалить профайл
Отчёт