

Режимы работы ключевых носителей Рутокен с КриптоПро CSP

- Названия режимов работы
- Ключевые носители Рутокен и поддерживаемые ими режимы работы
- Использование Пассивного режима
- Использование Активного режима
- Использования ФКН режима

Названия режимов работы

Самым безопасным вариантом хранения контейнера с сертификатом и ключом электронной подписи (ЭП) является ключевой носитель, защищенном PIN-кодом. Такие носители существуют в двух более распространенных форм-факторах: USB-токен и смарт-карта.

Для носителей Рутокен существуют следующие режимы работы с КриптоПро CSP:

- **Пассивный (Режим CSP).** Контейнер генерируется через программный криптопровайдер КриптоПро CSP. В таком режиме контейнер с ключом ЭП и сертификатом хранится на токене или смарт-карте и передается криптопровайдеру, работающему в операционной системе, который уже решает, что с ним делать. Такой контейнер будет неэкспортируемым, если при его создании будут выполнены специальные настройки. Если контейнер будет создан как экспортируемый, то его можно скопировать на другой носитель. Данный режим создает *извлекаемые ключи*.
- **Активный (Активный токен без защиты канала).** Контейнер генерируется при помощи внутреннего криптоядра Рутокена семейства ЭЦП, с использованием библиотеки PKCS#11. В таком режиме контейнер тоже хранится на токене или смарт-карте. Отличие в том, что пользователь может получить от этого носителя результат выполнения криптографических операций с использованием хранимого на устройстве закрытого ключа, поэтому такие ключи нельзя украсть или скопировать. В данном случае *ключ является неизвлекаемым*. Активные носители имеют возможность хранить контейнеры в пассивном режиме, что снижает безопасность ключа.
- **Функциональный ключевой носитель (Режим ФКН с защитой канала).** В таком режиме добавлена поддержка работы с неизвлекаемыми ключами по протоколу SESPAKE. Этот протокол позволяет реализовать процесс аутентификации не передавая PIN-код в открытом виде. Также SESPAKE позволяет установить зашифрованный канал для обмена сообщениями между криптопровайдером и носителем. Устройства типа ФКН можно использовать как устройства типа Активный и Пассивный.

Ключевые носители Рутокен и поддерживаемые ими режимы работы

Каждый Рутокен работает в одном, двух или трех режимах.

В таблице указаны носители, продемонстрировавшие работоспособность с соответствующими версиями КриптоПро CSP.

На пересечении строки с названием модели Рутокена и строки с версией КриптоПро CSP указаны режимы работы носителя.

Модель Рутокена	Версия КриптоПро CSP			
	4.0 R4	5.0 11455	5.0 R2 12000 (в т.ч. сборка с PKCS#11 модулями)	5.0 R3
Рутокен S Рутокен Lite	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)
Рутокен ЭЦП 2.0 2100 / Рутокен ЭЦП 2.0 (2000) / Рутокен ЭЦП 2.0 Flash / Рутокен ЭЦП Bluetooth	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)
		Режим Активный токен без защиты канала (rutoken_crypt)	Режим Активный токен (pkcs11_rutoken_esc)	Режим Активный токен (pkcs11_rutoken_esc)
Рутокен 2151 / Смарт-карта Рутокен 2151	Не поддерживается	Не поддерживается	Пассивный (Режим CSP)	Пассивный (Режим CSP)
			Режим Активный токен (pkcs11_rutoken_esc)	Режим Активный токен (pkcs11_rutoken_esc)

Рутокен ЭЦП PKI	Не поддерживается	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)
Рутокен ЭЦП 2.0 3000	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)
Рутокен ЭЦП 3.0 3100		Режим ФКН с защитой канала (rutoken_fkc)	Режим Активный токен (pkcs11_rutoken_escr)	Режим Активный токен (pkcs11_rutoken_escr)
Рутокен ЭЦП 3.0 3220			Режим ФКН с защитой канала (rutoken_fkc)	Режим ФКН с защитой канала (rutoken_fkc)
Рутокен ЭЦП 3.0 NFC 3100	Не поддерживается	Не поддерживается	i O S v i P a d OS	Режим ФКН с защитой канала (rutoken_fkc_nfc)
Смарт-карта Рутокен ЭЦП 3.0 NFC 3100				Режим Активный токен (pkcs11_rutoken_escr)
(бесконтактное (NFC) подключение)				Пассивный (Режим CSP)
			A n d r oid	Режим ФКН с защитой канала (rutoken_fkc_nfc)
				Режим Активный токен (pkcs11_rutoken_escr)
				Пассивный (Режим CSP)
			A v r o p a	Режим ФКН с защитой канала (rutoken_fkc_nfc)
			H a s t o l ь н ы е ПК	Режим ФКН с защитой канала (rutoken_fkc_nfc)
				Режим Активный токен (pkcs11_rutoken_escr)
				Пассивный (Режим CSP)
Рутокен ЭЦП 3.0 NFC 3100	Не поддерживается	Не поддерживается	Пассивный ¹ (Режим CSP)	
(контактное подключение)			Режим Активный токен ^{1, 2} (pkcs11_rutoken_escr)	
			Режим ФКН с защитой канала (rutoken_fkc)	
Смарт-карта Рутокен ЭЦП 3.0 NFC 3100	Не поддерживается	Не поддерживается	Пассивный ¹ (Режим CSP)	
(контактное подключение)			Пассивный ¹ (Режим CSP)	

			Режим Активный токен 1, 2 (pkcs11_rutoken_еср)	Режим Активный токен 1 (pkcs11_rutoken_еср)
			Режим ФКН с защитой канала (rutoken_fkc_nfc)	Режим ФКН с защитой канала (rutoken_fkc_nfc)
Смарт-карта Рутокен ЭЦП 2.0 2100	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)	Пассивный (Режим CSP)
		Режим Активный токен без защиты канала (rutoken_crypt)	Режим Активный токен (pkcs11_rutoken_еср)	Режим Активный токен (pkcs11_rutoken_еср)

¹ не работает в ОС Android и iOS

² не поддерживается в ОС Аврора

Использование Пассивного режима

[Хранение ЭП в защищенной файловой системе Рутокен](#)

Устройства в режимах Активный и ФКН можно использовать как устройства в режиме Пассивные. Но это значительно снижает защищенность ключа эл. подписи.

Использование Активного режима

Подписание документов будет происходить на неизвлекаемых аппаратных ключах. Этот режим предотвращает извлечение ключа в память компьютера в момент подписания.

Устройства в режиме ФКН можно использовать как устройства в режиме Активный.

[Генерация неизвлекаемых ключей на Рутокенах в КриптоПро CSP 5.0](#)

[Генерация неизвлекаемых ключей на Рутокенах в КриптоПро CSP 5.0 R2](#)

Использования ФКН режима

В КриптоПро CSP и Рутокенах с поддержкой ФКН реализован криптографический протокол SESPake. При работе будет устанавливаться зашифрованный канал для обмена сообщениями между криптопровайдером и носителем.

[Генерация контейнера ФКН на Рутокен ЭЦП 2.0 3000 с помощью КриптоПро CSP 5.0](#)

[Как проверить, что ключи на Рутокен ЭЦП 2.0 3000 сгенерированы в формате ФКН?](#)

[Генерация контейнера ФКН на смарт-карте Рутокен ЭЦП 3.0 NFC с помощью КриптоПро CSP 5.0 R2](#)

[Как проверить, что ключи на смарт-карте Рутокен ЭЦП 3.0 NFC сгенерированы в формате ФКН?](#)