



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

КриптоПро без техника: наш стандарт для 1С и банка

CSP 5.0 R3, переход на ГОСТ-2018, токены, цепочка доверия и плагин на 10-50 мест

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

К нам приходят в день сдачи: 1С:Отчётность не подписывает декларацию, клиент-банк не пускает по сертификату, ЭДО отдаёт «Не удалось построить цепочку». Причина почти всегда одна из четырёх: ветка CSP старше 5.0 R2 и не тянет ГОСТ-2018, слетела привязка лицензии, контейнер лежал в реестре профиля, нет корневых ГУЦ и УЦ ФНС. Закрываем это регламентом, а не разовым ремонтом.

Почему это важно бизнесу

- Срыв срока сдачи отчётности: штраф и блокировка счёта считаются от даты приёма, а не от даты попытки подписать
- Встают платежи: без рабочего СКЗИ не уходят зарплата, налоги и оплата поставщикам в тот же день
- Стоит ЭДО и маркировка: приёмка накладных и вывод из оборота в Честном ЗНАКе останавливаются целиком
- Клиентская лицензия CSP на терминальном сервере — нарушение условий поставки и риск при аудите ПО
- Утрата контейнера из реестра без копии = перевыпуск сертификата в УЦ: минимум сутки простоя подписанта

Ключевые параметры реализации

5.0 R3

ветка КриптоПро CSP по умолчанию: Windows 11 и Windows Server 2022, ГОСТ-2018

документация КриптоПро CSP

01.04.2026

ФНС перешла на ГОСТ 34.12-2018 и 34.13-2018: нужна CSP 5.0 R2 и выше

материалы ФНС России

15 мес

срок сертификата УЦ ФНС; перевыпуск планируем за 30 дней до истечения

регламент УЦ ФНС России

3.0 / SE

носители под новые ГОСТы: Рутокен ЭЦП 3.0, JaCarta-2 SE; ЭЦП 2.0 выводим

требования к носителям УЦ ФНС

2 звена

цепочка доверия: ГУЦ Минцифры → УЦ ФНС России → сертификат организации

наш чеклист развёртывания

0 в реестре

контейнеров в реестре профиля не оставляем: закрытый ключ живёт на токене

наш стандарт внедрения



Бухгалтерия на RDS: подпись видна в панели, но не видна в 1С

Что настраиваем

Бухгалтерская фирма, 12 рабочих мест, 1С:Бухгалтерия на Windows Server 2019, токены у пользователей на своих ПК

Как мы это делаем

- 1 На самом сервере в сессии пользователя: `csptest -keyset -enum_cont -verifycontext -fqcn` — контейнер токена виден, значит проброс живой
- 2 `certmgr -list -store uMy` пуст: личный сертификат стоял в mMy, в хранилище компьютера, поэтому 1С под пользователем его не находила
- 3 Ставим сертификат из контейнера в uMy, проверяем «Путь сертификации»: корневой ГУЦ Минцифры в Root, сертификат УЦ ФНС в CA
- 4 В 1С: Администрирование → Обмен электронными документами → Настройки ЭП и шифрования — заново добавляем программу КриптоПро CSP и сертификат
- 5 В RDP включаем перенаправление смарт-карт, а не USB-устройства: проверяем службу SCardSvr и запрещающую политику перенаправления

РЕЗУЛЬТАТ

Подпись отчётности и ЭДО заработали в тот же день, без перевыпуска сертификата и без обращения в УЦ. Мы закрепили правило: на RDS сертификаты ставим только в хранилище пользователя, а проверку делаем утилитами на сервере, а не «на глаз» в панели на клиентском ПК.

КЛЮЧЕВОЙ НЮАНС

Контейнер и сертификат — разные сущности и разные хранилища. Диагностику начинаем с `csptest` и `certmgr` в сессии того самого пользователя: это сразу отделяет проблему проброса от проблемы хранилища.



После обновления ОС встали клиент-банк и 1С:Отчётность

Что настраиваем

Оптовая торговля, 28 рабочих мест, два подписанта, контейнеры исторически хранились в реестре профиля Windows

Как мы это делаем

- 1 Обновление ОС и переезд профиля: ветка HKLM\SOFTWARE\Wow6432Node\CryptoPro\Settings\Users\<SID>\Keys для нового SID оказалась пуста
- 2 Лицензия CSP: привязка слетела после смены оборудования, смотрим её в srconfig и вводим серийный номер из нашего реестра лицензий
- 3 Перевыпускаем оба сертификата в УЦ ФНС на Рутокен ЭЦП 3.0, реестровые контейнеры выводим из эксплуатации полностью
- 4 Портал банка работает по TLS с ГОСТ-шифрсыютами: ставим браузер с их поддержкой и проверяем вход до реального платежа
- 5 Плагин ЭЦП Browser plug-in и расширение CAdES включаем, тестовую подпись делаем на демостранице вендора, а не на платёжке

РЕЗУЛЬТАТ

Платежи ушли в тот же операционный день. С тех пор у клиента ни одной потери ключа при обновлениях: закрытый ключ физически не зависит от профиля Windows, а серийники лицензий не приходится искать по почте задним числом.

КЛЮЧЕВОЙ НЮАНС

Реестровый контейнер живёт ровно до первого переезда профиля. Ключ на сертифицированном носителе и учтённый серийник лицензии — две строчки регламента, которые снимают целый класс аварий.



Подводные камни

✗ Осталась ветка CSP 4.0

Поддержка ветки 4.0 прекращена, ГОСТ 34.12-2018 она не умеет. Для обмена с ФНС нужна 5.0 R2 и выше, наш стандарт — 5.0 R3.

✗ Установка поверх старой версии

Остаются компоненты прежней ветки. Корректно: удаление, перезагрузка, установка новой версии, снова перезагрузка.

✗ Сертификат в хранилище компьютера

1С и браузер работают с личным хранилищем пользователя (uMy). Сертификат, поставленный в mMy, приложению просто не виден.

✗ Нет корневых ГУЦ и УЦ ФНС

Подпись помечается недоверенной. Корневой ГУЦ Минцифры — в «Доверенные корневые», сертификат УЦ ФНС — в «Промежуточные».

✗ Клиентская лицензия на RDS

Для терминального сервера нужна серверная лицензия CSP. Иначе ошибки лицензирования в самый пик отчётности.

✗ Контейнер в реестре без копии

Переезд профиля или переустановка ОС уничтожают ключ безвозвратно — остаётся только перевыпуск в удостоверяющем центре.

✗ Носитель снят с сертификации

На Рутокен ЭЦП 2.0 новые ключи не записывают: сертификат ФСБ на встроенное СКЗИ истёк. Берём Рутокен ЭЦП 3.0 или JaCarta-2 SE.

✗ Плагин поставили, расширение — нет

В Chromium-браузерах нужно ещё включить расширение CryptoPro Extension for CAdES Browser Plug-in и перезапустить браузер.

Как правильно

МИНИМУМ

- КриптоПро CSP 5.0 R2 и выше, установка от администратора, затем перезагрузка
- Личный сертификат — в uMy, корневые ГУЦ и УЦ ФНС — в Root и CA
- Тестовая подпись файла до реального документа, платежа и сдачи отчёта
- Реестр лицензий: серийник, машина, пользователь, дата истечения

НОРМАЛЬНО

- Закрытые ключи на сертифицированных носителях: Рутокен ЭЦП 3.0, JaCarta-2 SE
- Серверные лицензии CSP на RDS и перенаправление смарт-карт в профиле RDP
- Корневые сертификаты и списки отзыва раздаём групповой политикой домена
- Плагин и расширение браузера ставим централизованно, версию фиксируем

ХОРОШО

- Календарь перевыпуска: напоминание за 30 дней до конца 15-месячного срока
- Тестовый стенд: проверяем обновление CSP и ОС до раскатки на подписантов
- Мониторинг служб СКЗИ и доступности точек CDP и OCSP удостоверяющих центров
- Регламент передачи носителя при отпуске и увольнении подписанта

Чек-лист самопроверки

- | | |
|--|---|
| ☐ Версия CSP не ниже 5.0 R2, наш стандарт 5.0 R3, а ОС есть в списке поддержки вендора | ☐ Лицензия CSP действующая и соответствует типу места: клиентская на ПК, серверная на RDS |
| ☐ Старая ветка CSP удалена до установки, между удалением и установкой сделана перезагрузка | ☐ Носитель актуальный: Рутокен ЭЦП 3.0 или JaCarta-2 SE, ключ записан самим удостоверяющим центром |
| ☐ <code>csptest -keyset -enum_cont -verifycontext -fqcn</code> показывает контейнер в сессии нужного пользователя | ☐ ЭЦП Browser plug-in установлен, расширение CAdES включено, демостраница вендора подписывает |
| ☐ <code>certmgr -list -store uMy</code> подтверждает личный сертификат у пользователя, а не только в mMy | ☐ В 1С добавлены программа КриптоПро CSP и сертификат, тестовая подпись проходит без ошибок |
| ☐ «Путь сертификации» построен целиком: ГУЦ Минцифры → УЦ ФНС России → организация | ☐ Клиент-банк проверен реальным запросом выписки, а не только входом в личный кабинет |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем СКЗИ по регламенту: версия, хранилища, цепочка доверия, проброс носителей на RDS
- Переводим парк на CSP 5.0 R2 и выше и на носители под новые ГОСТы до отказа обмена с ФНС
- Ведём реестр лицензий и сертификатов клиента, заранее готовим перевыпуск до истечения срока
- Настраиваем подпись в 1С:Отчётности, 1С:ЭДО, маркировке и клиент-банке с проверкой на тесте
- Разбираем аварии подписи по шагам: службы, лицензия, контейнер, цепочка, плагин, проброс RDP

15+

лет в ИТ-поддержке

50

рабочих мест — наш профиль

МТС

дата-центр, Москва



КОНТАКТЫ

Обсудить вашу задачу

Сайт **itfresh.ru**

Телефон **+7 903 729-62-41**

Telegram **@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.



itfresh.ru



Техническая база

- 01** КриптоПро CSP: руководство администратора безопасности (docs.cryptopro.ru — 5.0 R3)
- 02** КриптоПро ЭЦП Browser plug-in: установка и настройка браузеров (docs.cryptopro.ru — 2026)
- 03** Удостоверяющий центр ФНС России: порядок получения КЭП (nalog.gov.ru — 2026)
- 04** ФНС России: переход на ГОСТ 34.12-2018 и ГОСТ 34.13-2018 (nalog.gov.ru — 2026)
- 05** Головной УЦ Минцифры: корневые сертификаты и списки отзыва (e-trust.gosuslugi.ru — 2026)
- 06** 1С:ИТС — электронная подпись, 1С:Отчётность и 1С:ЭДО (its.1c.ru — 2026)
- 07** Microsoft Learn: хранилища сертификатов и CryptoAPI в Windows (learn.microsoft.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

