



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

КЭП на рабочих местах: стек КриптоПро без боли

Как мы разворачиваем CSP 5.0 R4, токены, плагин и
подписание в RDP на парке до 50 РМ

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Подпись ломается не «вдруг»: криптопровайдер, драйвер токена, браузерный плагин и цепочка доверия — четыре независимых продукта, и обновление любого рвёт связку. Мы приводим парк к одной конфигурации: КриптоПро CSP 5.0 R4, ровно один драйвер токена, плагин 2.0 плюс расширение, корневой и промежуточные сертификаты УЦ в ROOT и CA. Иначе бухгалтерия встаёт в отчётный день.

Почему это важно бизнесу

- Срыв срока сдачи отчётности из-за неработающей подписи — это пени и блокировка счёта, а не «неудобство ИТ».
- Простой бухгалтера в отчётный период стоит дороже серверной лицензии КриптоПро на терминальный сервер.
- Сертификат КЭП от УЦ ФНС действует 15 месяцев: пропущенный перевыпуск = поездка в инспекцию и остановка ЭДО.
- Один токен — один руководитель: при смене директора КЭП не передаётся, нужен новый выпуск и пересбор доступов.
- Разнобой версий CSP и драйверов превращает каждый инцидент в часовую диагностику вместо пятиминутной.

Ключевые параметры реализации

5.0 R4

Целевая версия КриптоПро CSP на парке: одна для всех АРМ и терминальных серверов

документация КриптоПро CSP

5.0.13600

Эталонная сборка 5.0 R4 и новее: одинаковая на всех АРМ и в образе терминального хоста

релиз КриптоПро CSP 5.0 R4

15 мес.

Срок действия сертификата КЭП, выданного УЦ ФНС; напоминание о перевыпуске — за 45 дней

порядок УЦ ФНС + наш стандарт

10 попыток

Предел и значение по умолчанию для попыток ввода PIN на Рутокене; задаётся при форматировании

документация Рутокен: PIN-коды

1 драйвер

Ровно один клиент токена на АРМ: Драйверы Рутокен 5.2 или Единый Клиент JaCarta, не оба

наш стандарт эталона АРМ

2 хранилища

Корневой УЦ в ROOT, промежуточные в CA; раскатываем certutil -addstore через GPO

документация Microsoft: certutil

Эталон APM: CSP 5.0 R4, драйвер токена и плагин

Что настраиваем

Все Windows-APM, где подписывают: бухгалтерия, юристы, руководитель; развёртывание скриптом и GPO от имени SYSTEM

Как мы это делаем

- 1 Снимаем инвентарь: версия CSP, установленные драйверы токенов, плагин и расширение; лишнее — второй клиент токена, старый CSP 4.0 — удаляем до установки.
- 2 Ставим драйвер токена первым: комплект «Драйверы Рутокен для Windows» 5.2 с Панелью и Центром управления Рутокен либо Единый Клиент JaCarta — строго один продукт на...
- 3 Разворачиваем КриптоПро CSP 5.0 R4 тихо: `msiexec /i csp-x64.msi /qn /norestart /l*v csp.log`, серийный номер лицензии вносим отдельным шагом, затем плановая перезагр...
- 4 Ставим КриптоПро ЭЦП Browser plug-in 2.0 и отдельно расширение CryptoPro Extension for CAdES Browser Plug-in — без пары кнопка подписи неактивна.
- 5 Проверяем демо-страницей `cades_bes_sample.html` на `cryptopro.ru` и командой `csptest -keyset -enum_cont -fqcn -verifycontext:` контейнер виден — APM принят.

РЕЗУЛЬТАТ

Новое рабочее место собирается по одному скрипту, а не «как получится». Инциденты сводятся к трём проверяемым точкам: версия CSP, единственный драйвер, пара плагин плюс расширение. Диагностика чужой машины перестаёт быть археологией.

КЛЮЧЕВОЙ НЮАНС

Порядок «драйвер → CSP → токен → сертификат» и перезагрузка после установки CSP — не суеверие: часть компонентов провайдера подхватывается только после рестарта. Состав считывателей проверяем в панели «КриптоП...



Цепочка доверия: корни и промежуточные УЦ в хранилищах

Что настраиваем

Все АРМ и RDS-хосты, где всплывает «Сертификат не является доверенным» в СБИС, Диадоке и на госпорталах

Как мы это делаем

- 1 Забираем с сайта своего УЦ корневой и промежуточные сертификаты и храним их в репозитории рядом с эталоном АРМ, а не «скачиваем каждый раз руками».
- 2 Раскатываем массово: `certutil -addstore root <файл>` для корневого и `certutil -addstore ca <файл>` для промежуточных, из-под администратора машины.
- 3 Личный сертификат ставим из контейнера токена с привязкой к ключу: в панели CSP «Установить личный сертификат» либо `certmgr -inst -file cert.cer -store uMy -cont <к...`
- 4 Госкорни добавляем туда же — иначе ГОСТ-порталы отдадут белый экран; для таких площадок держим Chromium-Gost, он работает через msspi поверх CSP 5.0.
- 5 Контроль: `certutil -store root` и `certutil -store ca` в отчёте инвентаризации, отдельная проверка срока — сертификат КЭП от УЦ ФНС действует 15 месяцев.

РЕЗУЛЬТАТ

Ошибка «сертификат не является доверенным» уходит как класс: цепочка строится локально, без похода на сайт УЦ в момент подписания. Новый АРМ и новый терминальный сервер получают полный набор корней при развёртывании, а не после первой жалобы.

КЛЮЧЕВОЙ НЮАНС

Windows строит цепочку до корня сам, но только по тому, что лежит в ROOT и CA. Промежуточный сертификат в «Личных» не считается: раскладывать надо строго по хранилищам, иначе подпись невалидна.



Подпись в RDP: перенаправление токена и лицензии

Что настраиваем

Терминальные серверы с 1С и ЭДО, где токен физически у бухгалтера, а подписание идёт в сессии на сервере

Как мы это делаем

- 1 Ставим драйвер токена и КристоПро CSP на сам RDS-хост: без клиента считывателя устройство в сессии не появится, сколько ни пробрасывай.
- 2 Включаем перенаправление смарт-карт: в mstsc «Локальные ресурсы» → «Подробнее» → «Смарт-карты», на хосте политика Do not allow smart card device redirection — Disab...
- 3 Для токенов, не видимых как смарт-карта, включаем клиентскую политику Allow RDP redirection of other supported RemoteFX USB devices from this computer — она задаётся...
- 4 Лицензию берём серверную: на серверной ОС клиентская лицензия CSP не работает вовсе, а серверная выдаётся на сервер и не считает пользователей.
- 5 Альтернатива при ограничениях проброса — USB-over-IP с последовательным доступом к токenu; выбор фиксируем в регламенте, а не решаем по случаю.

РЕЗУЛЬТАТ

Бухгалтер подписывает из дома тем же токеном, что и в офисе, а ключи не расползаются россыпью по серверу. Ошибки вида «не найден действующий сертификат» на RDS исчезают — они почти всегда про отсутствие серверной лицензии и драйвера токена на хосте.

КЛЮЧЕВОЙ НЮАНС

Проброс USB и перенаправление смарт-карт — разные механизмы RDP с разными политиками, причём RemoteFX USB настраивается на клиенте, а запрет смарт-карт — на хосте. Сначала выясняем, каким классом устройства то...



Подводные камни

✗ Два клиента токена на одной машине

Драйверы Рутокен и Единый Клиент JaCarta делят считыватели и конфликтуют. Оставляем один продукт, лишний удаляем до установки CSP.

✗ Поставили расширение, забыли плагин

Плагин ставится в систему, расширение — в браузер; это два компонента. Без пары кнопка подписи остаётся неактивной без внятной ошибки.

✗ Промежуточный сертификат в «Личных»

Цепочка не строится: Windows ищет промежуточные только в СА. Раскладываем certutil -addstore ca, корневой — certutil -addstore root.

✗ Работа на триале КристоПро

Пробный период молча заканчивается, и подпись «ломается» без изменений в системе. Лицензию вносим на этапе развёртывания и учитываем.

✗ Клиентская лицензия на RDS

На серверной ОС клиентская лицензия CSP не действует, включая встроенную в сертификат. Нужна серверная — одна на сервер, без ограничения числа пользо...

✗ Блокировка токена неверным PIN

Лимит попыток задаётся при форматировании токена, максимум 10. Разблокировка — PIN-кодом администратора; при его потере ключ теряется вместе с носителем...

✗ Пропущенный перевыпуск сертификата

Сертификат КЭП от УЦ ФНС действует 15 месяцев. Ведём календарь: после истечения дистанционный перевыпуск в личном кабинете недоступен, нужен визит в...

✗ «КЭП не принимается на Госуслугах»

Это не КристоПро: либо подпись не того лица, либо полномочия не делегированы в ЕСИА, либо нет МЧД, подписанной КЭП руководителя.



Как правильно

МИНИМУМ

- Один драйвер токена, КриптоПро CSP 5.0 R4 с лицензией, плагин 2.0 плюс расширение
- Корневой и промежуточные сертификаты УЦ в хранилищах ROOT и CA на каждом АРМ
- Календарь перевыпуска КЭП с напоминанием за 45 дней до конца 15 месяцев

НОРМАЛЬНО

- Единый эталон АРМ: тихая установка `msiexec /qn /norestart` и раскатка корней через GPO
- Инвентаризация версий CSP, драйверов и плагина в отчёте по всему парку
- Серверная лицензия CSP на RDS и явно настроенная политика перенаправления
- Chromium-Gost на машинах, работающих с порталами по ГОСТ-TLS

ХОРОШО

- Приёмка АРМ по чек-листу: демо-страница плагина и `csptest -keyset -enum_cont`
- МЧД и делегирование в ЕСИА оформлены заранее, а не в день сдачи отчётности
- Резервный сценарий подписания: второй токен сотрудника и запасное АРМ
- Мониторинг сроков сертификатов и лицензий CSP в общей системе учёта



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Версия КриптоПро CSP одинакова на всех АРМ и терминальных серверах и не ниже 5.0 R4? | ☐ Известна дата окончания каждого сертификата и назначен ответственный за перевыпуск? |
| ☐ Лицензия CSP постоянная, а не триал, и внесена в учёт по каждому рабочему месту? | ☐ На терминальном сервере есть серверная лицензия CSP (клиентская там не работает) и драйвер токена? |
| ☐ На машине установлен ровно один клиент токена — Рутокен или JaCarta, но не оба? | ☐ Политика перенаправления смарт-карт на хосте и RemoteFX USB на клиенте настроены осознанно? |
| ☐ Плагин КриптоПро ЭЦП Browser plug-in и расширение к нему стоят оба и проверены демо-страницей? | ☐ Для сотрудников оформлены МЧД и делегированы полномочия в ЕСИА? |
| ☐ Корневой сертификат УЦ лежит в ROOT, а промежуточные — в CA на каждой машине? | ☐ Есть план на случай блокировки токена: известен администраторский PIN и контакт УЦ? |

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).

- Собираем эталон рабочего места с КЭП и раскатываем его на весь парк скриптом и GPO
- Чистим конфликтующие драйверы токенов и приводим версии CSP и плагина к одной
- Разворачиваем цепочку доверия УЦ в ROOT и CA централизованно, без ручной установки
- Настраиваем подписание в RDP: перенаправление токена, драйверы на хосте, лицензии CSP
- Ведём календарь перевыпуска сертификатов, МЧД и лицензий и предупреждаем заранее

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 — описание продукта и поддерживаемые носители (cryptopro.ru — 5.0 R4)
- 02** КриптоПро ЭЦП Browser plug-in и демо-страница проверки подписи (cryptopro.ru — 2.0)
- 03** Приложение командной строки csptest и «Инструменты КриптоПро» (cptools) (cryptopro.ru — 5.0 R4)
- 04** Работа с PIN-кодами Рутокена и комплект драйверов для Windows (dev.rutoken.ru — 5.2)
- 05** certutil — управление хранилищами сертификатов Windows (learn.microsoft.com — 2026)
- 06** Device and Resource Redirection и RemoteFX USB — политики RDS (learn.microsoft.com — 2026)
- 07** Порядок получения сертификата КЭП в УЦ ФНС: срок 15 месяцев (nalog.gov.ru — 2026)
- 08** Chromium-Gost — браузер с поддержкой ГОСТ через msspi (cryptopro.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

