КРИПТОПРО

Ключевое слово
в защите информации

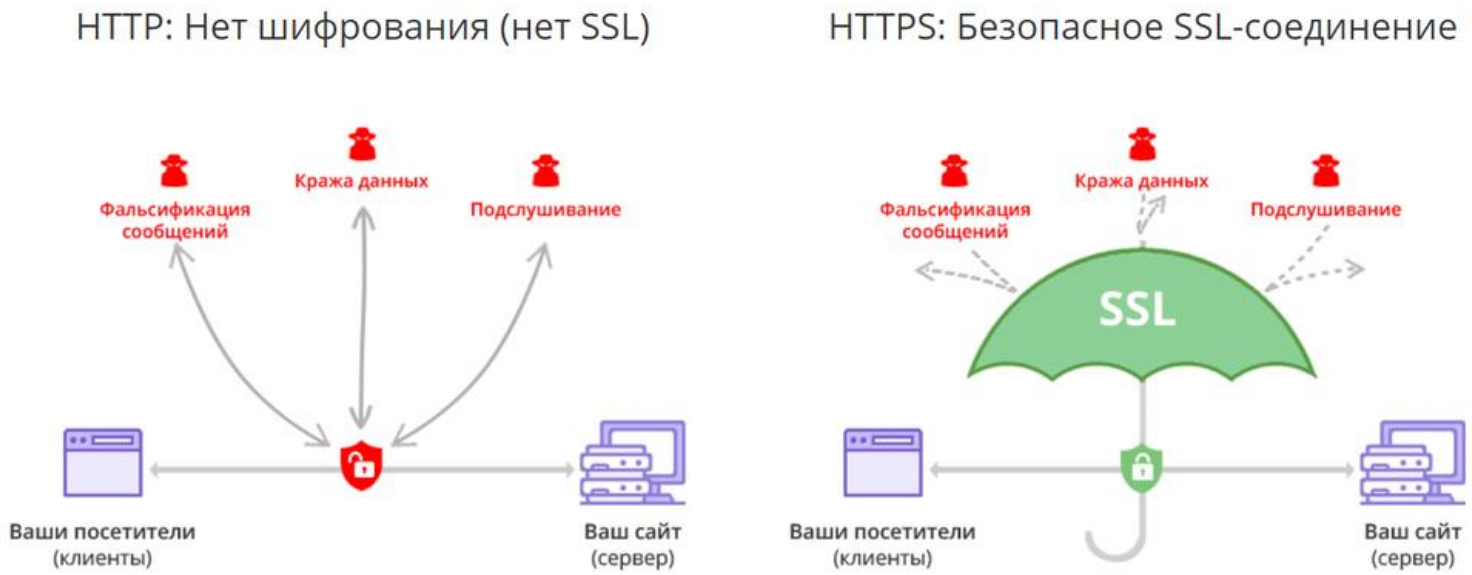
Защита доступа к веб-сайтам в условиях отзыва SSL(TLS)-сертификатов международными УЦ

Павел Луцик, Директор по развитию бизнеса и работе с партнерами

Павел Смирнов, Директор по развитию

18 марта 2022 года

Защищенные и незащищенные соединения



- HTTP – протокол **незащищенного** обмена данными между пользователем и сайтом
- HTTPS – расширение протокола HTTP, обеспечивающее **защиту** обмена данными
- SSL/TLS – протокол, реализующий защиту в HTTPS-соединении с помощью **сертификатов**
- ГОСТ TLS – протокол TLS с поддержкой **российских** алгоритмов шифрования, обеспечивающих надежную защиту передаваемых данных пользователя

Что такое TLS-сертификаты?

TLS-сертификат – эл.документ, выдаваемый Удостоверяющим Центром:

- Владельцам веб-сайтов (сертификат веб-сервера)
- Пользователям (персональный сертификат)

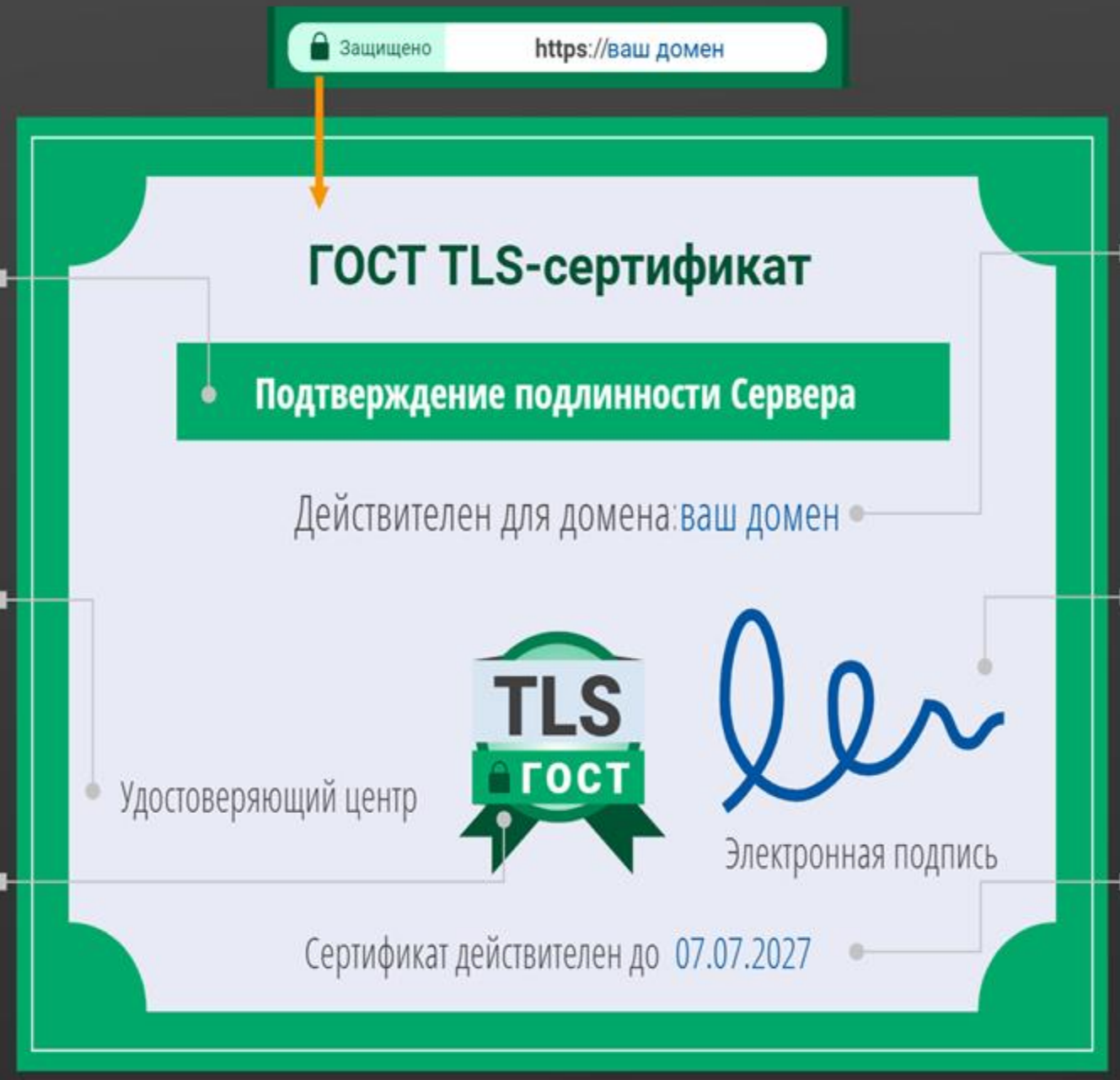
Сертификат веб-сервера является обязательным для TLS и защищает пользователя от:

- Фишинга (посещения поддельных сайтов)
- Внесения несанкционированных изменений в передаваемые данные
- Кражи передаваемой информации

Персональный сертификат не является обязательным для TLS и:

- Позволяет веб-серверу идентифицировать пользователя на сайте
- Может использоваться пользователем для эл.подписи

Формат TLS-сертификата



Сертификат подтерждает, что Сервер действительно тот, за кого себя выдаёт и его открытый ключ подлинный

Сертификат выписывается специализированным Удостоверяющим центром

Сертификат использует алгоритмы ГОСТ

Применение Сертификата ограничено выбранной доменной зоной

Сертификат подписывается электронной подписью Удостоверяющего центра, что защищает его от подделки

Сертификат имеет срок действия

Надежность инфраструктуры с TLS-сертификатами

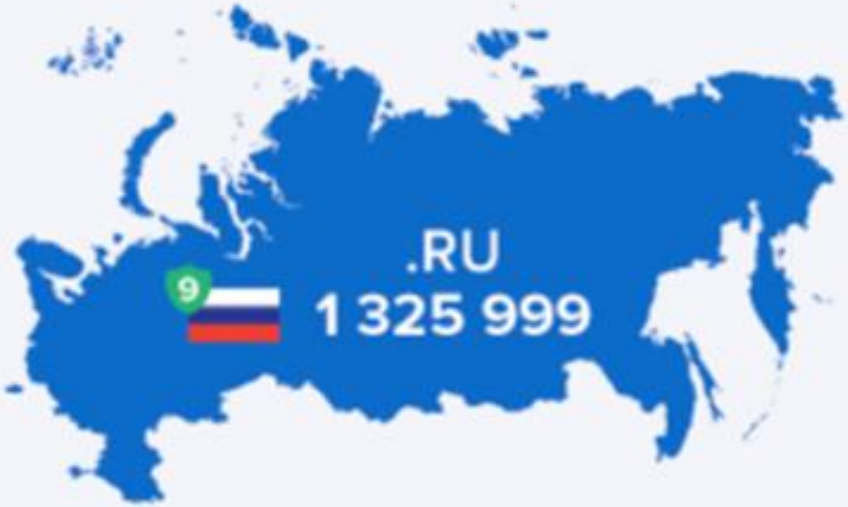
- Проверка всей цепочки эл.подписей TLS-сертификатов
- Проверка подлинности и «доверия» к корневому УЦ
- Проверка соответствия домена с записью в TLS-сертификате
- Проверка актуальности сертификата по утвержденному УЦ сроку действия
- Проверка применимости сертификата по списку отозванных сертификатов УЦ

Законодательное обеспечение ГОСТ TLS

- **2016.** Поручение Президента (Пр-1380) про переход ОГВ на российскую криптографию
- **2017.** Программа «Цифровая экономика РФ»
- **2018.** Дорожные карты по переходу на ГОСТ в Рунете
- **2020.** Пилотный проект по использованию российских алгоритмов и шифрсредств в ГИС
- **2022.** Ожидается принятие НПА по Национальному УЦ

ТОП-10 стран по количеству используемых TLS-сертификатов

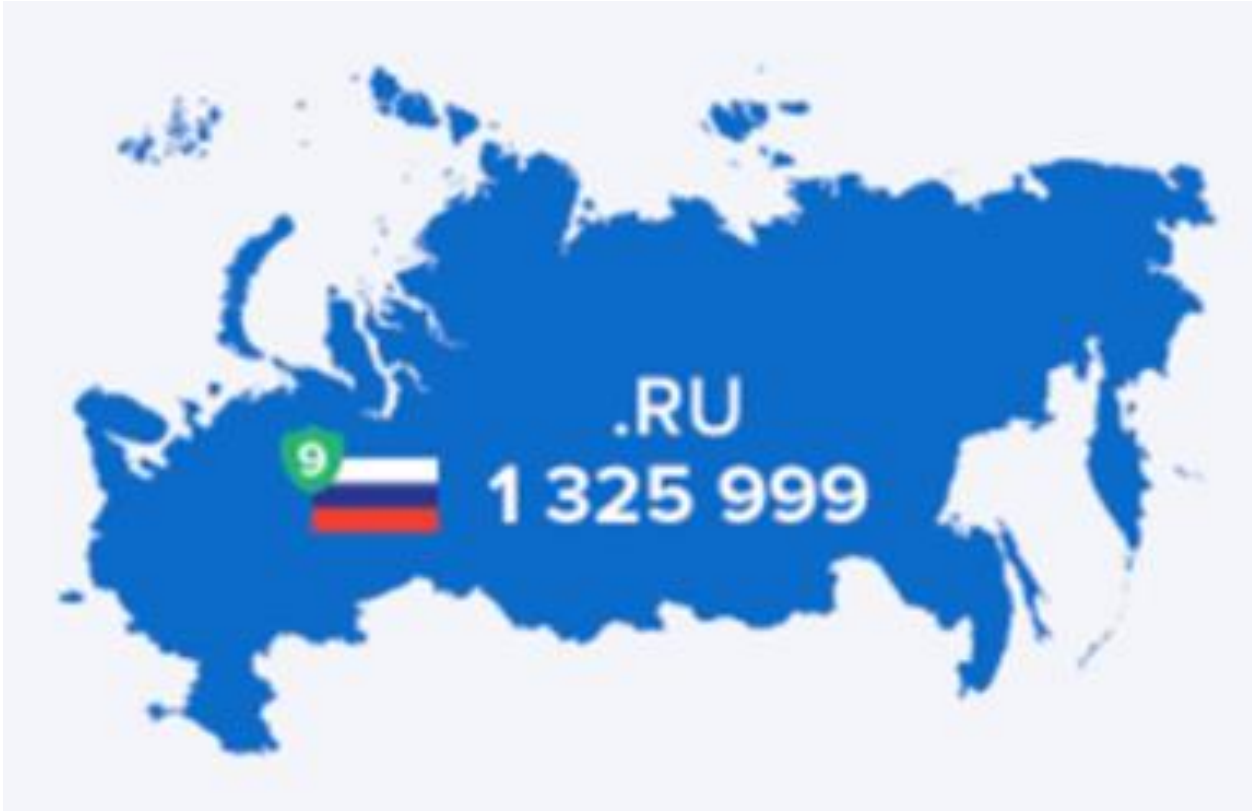
1. .US 45 619 376
2. .DE 6 841 157
3. .JP 2 410 826
4. .UK 2 397 158
5. .NL 2 215 705
6. .FR 2 058 494
7. .DK 1 607 158
8. .CA 1 407 358
9. .RU 1 325 999
10. .CN 1 115 118



По данным Netcraft за апрель 2020 года

ТОП-5 УЦ по количеству выпущенных SSL в .RU

- Let's Encrypt (960 000)
- CloudFlare (110 000)
- DigiCert (85 000)
- GlobalSign (75 000)
- Sectigo (55 000)



Риски использования TLS-сертификатов иностранных УЦ

Основные риски:

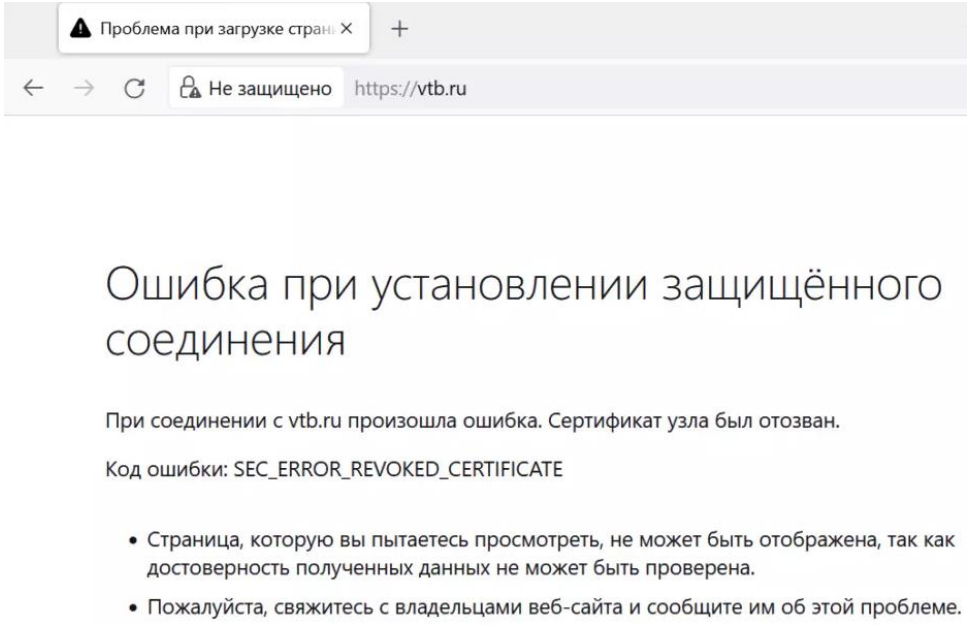
- Отзыв действующего сертификата
- Утрата доверия к корневому сертификату

Возможные последствия:

- Отключение защиты доступа пользователя к веб-сайту
- Оповещение пользователя браузером о недоверии к веб-сайту
- Блокировка доступа к сайту до специальных действий пользователя

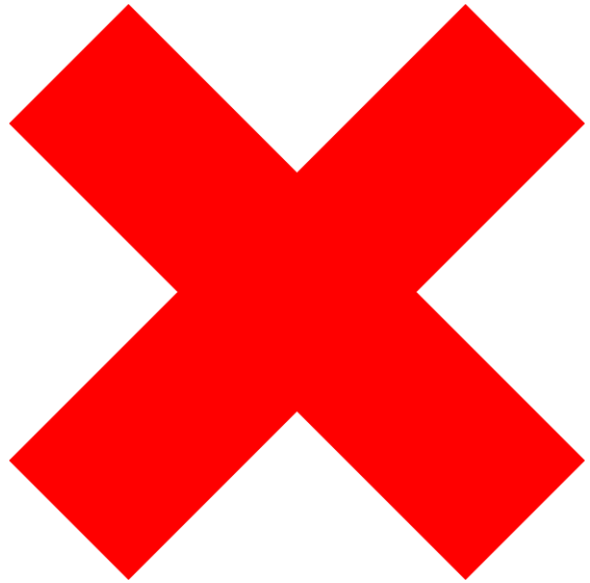
Отзыв и прекращение выдачи TLS-сертификатов

- 2017 – Утрата доверия Google к сертификатам от Symantec
- 2018 – Отозван сертификат Общественной Палаты РФ
- 2022 – Отозваны сертификаты ВТБ, ЦБ, ПСБ, Минобороны
- 2022 – Прекращена выдача сертификатов для Рунета со стороны УЦ Sectigo (бывш. Comodo), DigiCert, Thawte, Rapid, GeoTrust



Сомнительные варианты выхода из ситуации

- Перейти на небезопасный доступ по HTTP
- Отключить в браузерах проверку сертификатов
- Использовать самоподписанные сертификаты для каждого веб-сайта
- Отказаться от использования интернета



Временный вариант – TLS-сертификат лояльного (пока) зарубежного УЦ

Коммерческие зарубежные УЦ:

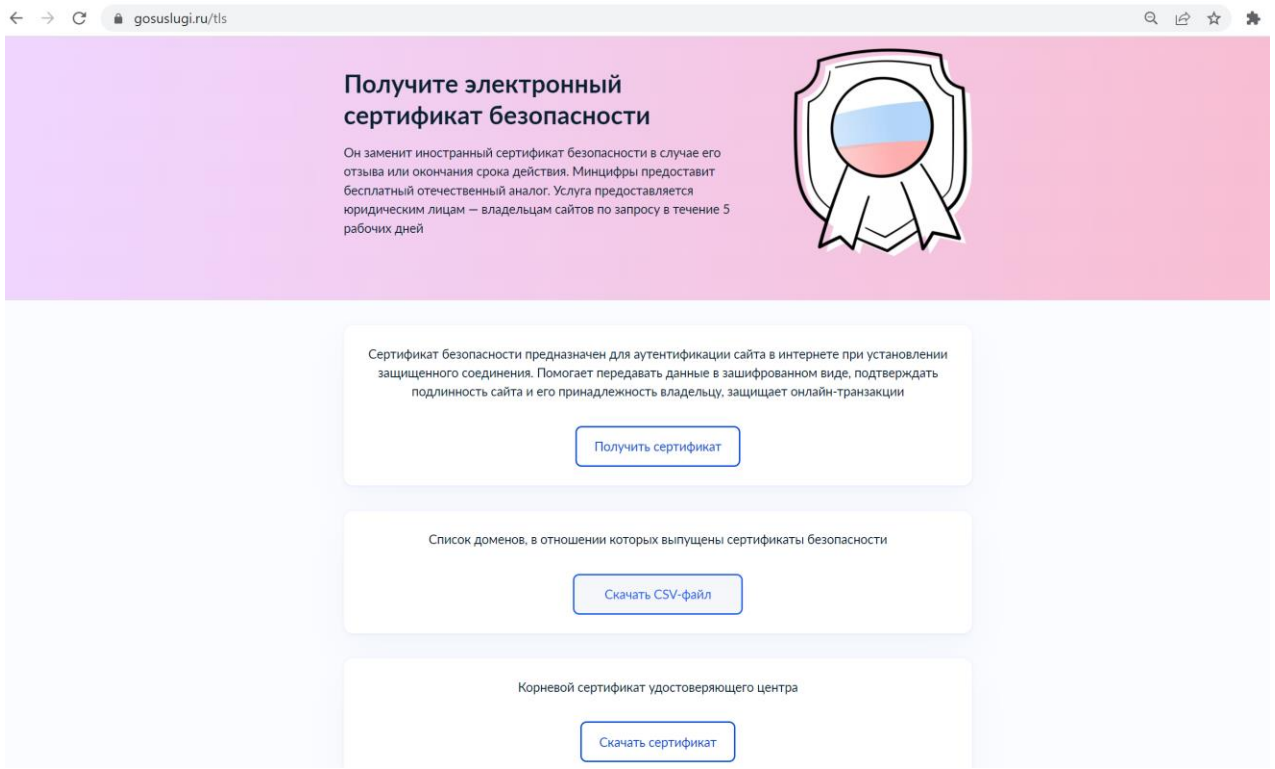
- Бельгия: https://www.globalsign.com
- Турция: https://e-tugra.com.tr/ssl-sertifikasi
- Италия: https://www.actalis.com/it/home.aspx
- Китай: https://www.cfca.com.cn/20150810/100002755.html

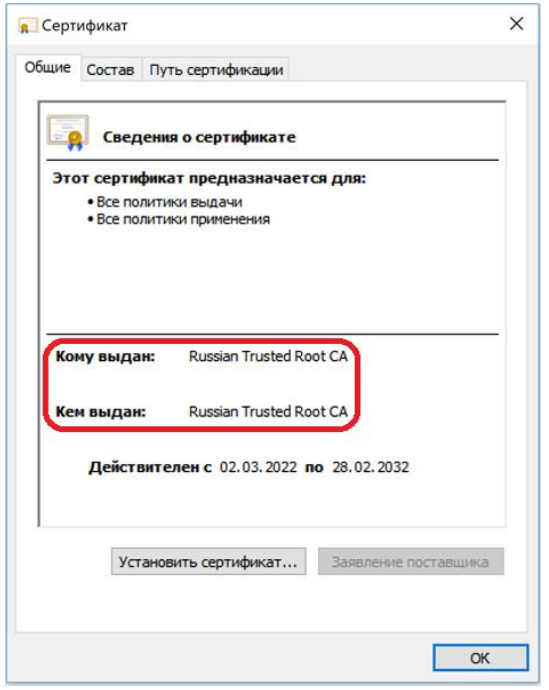
Некоммерческие зарубежные УЦ:

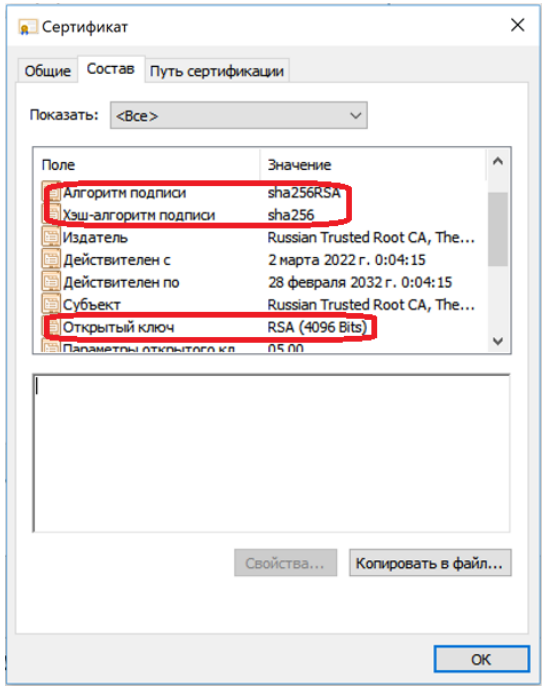
- Америка: https://letsencrypt.org
- Австрия: https://zerossl.com

Стандартный вариант – TLS-сертификат (RSA) от НУЦа

1. Юр.лицо (владелец сайта) отправляет подписанную заявку на Госуслуги
2. Минцифры проверяет принадлежность домена
3. Минцифры помещает домен в публичный список по адресу: www.gosuslugi.ru/tls
4. НУЦ выписывает RSA-сертификат на сайт





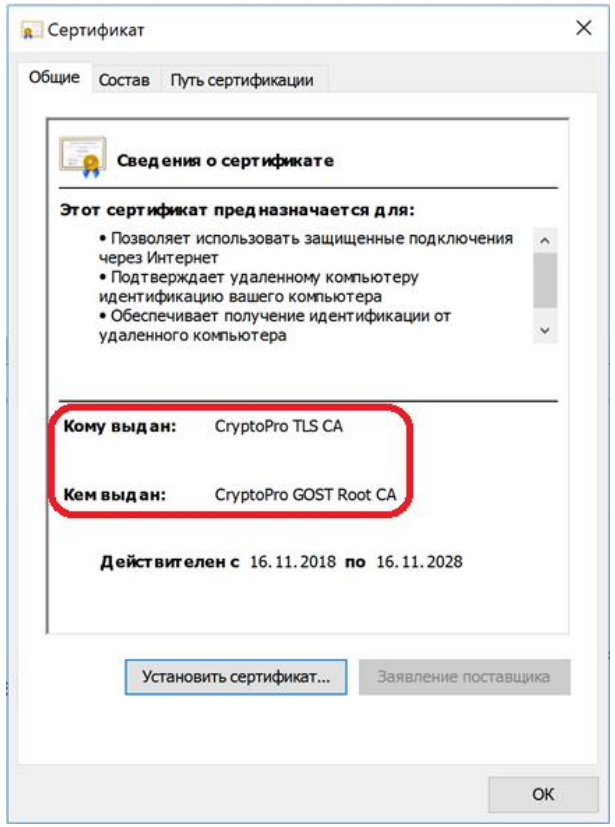


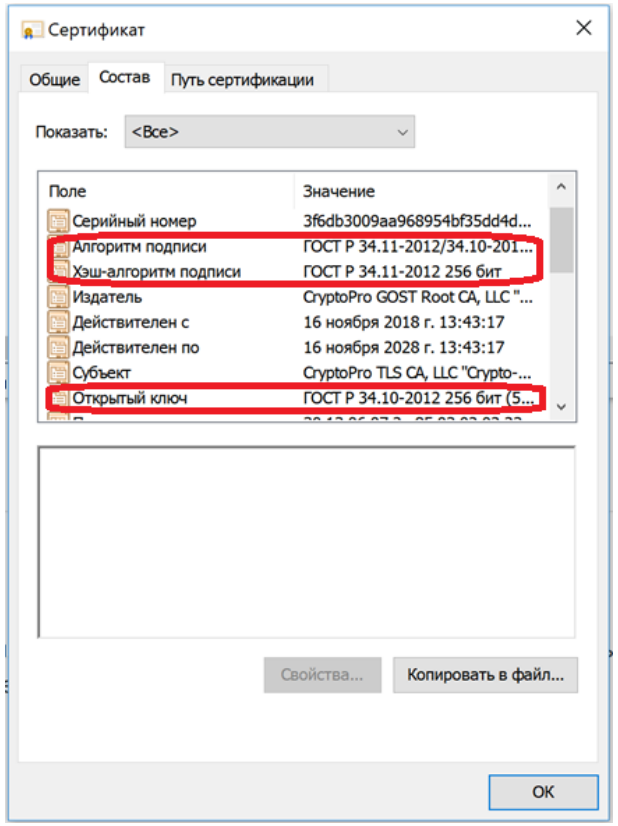
Доверие к сертификатам в браузерах

- В браузеры Яндекс и Атом добавлен корневой RSA-сертификат Минцифры
- Я.Браузер признает сертификаты НУЦ только для доменов из списка на сайте: www.gosuslugi.ru/tls
- Если посещаемого сайта нет в этом списке, отобразится стандартная ошибка и браузер не даст посетить сайт

Рекомендуемый диверсифицированный вариант – два TLS-сертификата (RSA и ГОСТ)

- Получить RSA-сертификат в УЦ Минцифры
- Получить ГОСТ-сертификат (например, тут: tlsca.cryptopro.ru/tls.htm)
- Использовать на веб-сайте одновременно два сертификата – RSA и ГОСТ





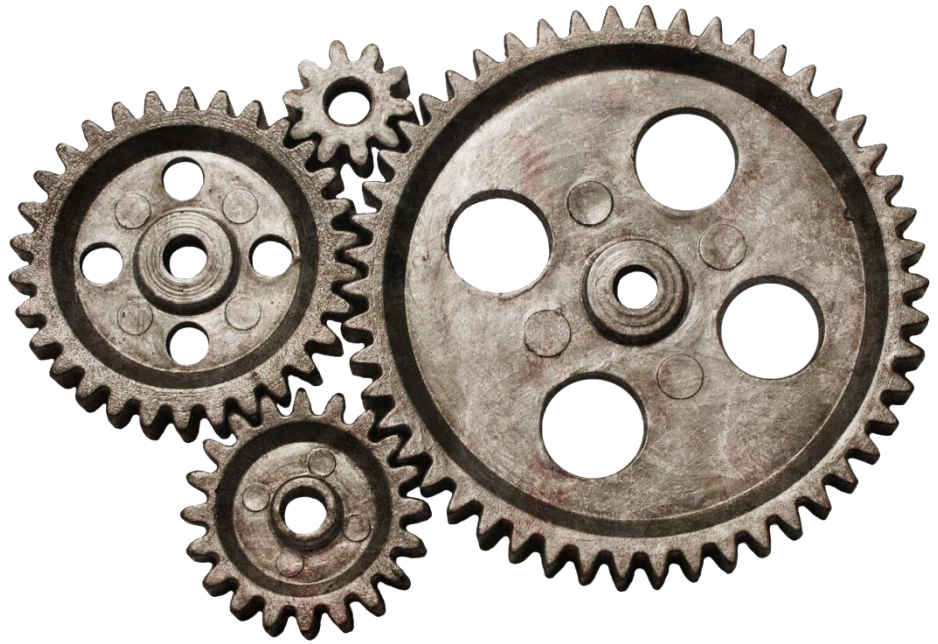
Доверие к корневым сертификатам в КриптоПро CSP

В промежуточную версию КриптоПро CSP 5.0 R3 (сборка 5.0.12417 Osiris) добавлена поддержка корневых сертификатов:

- RSA-сертификат Минцифры от 2022 года
- ГОСТ-сертификат CryptoPro TLS CA

Требуемые компоненты для работы ГОСТ TLS

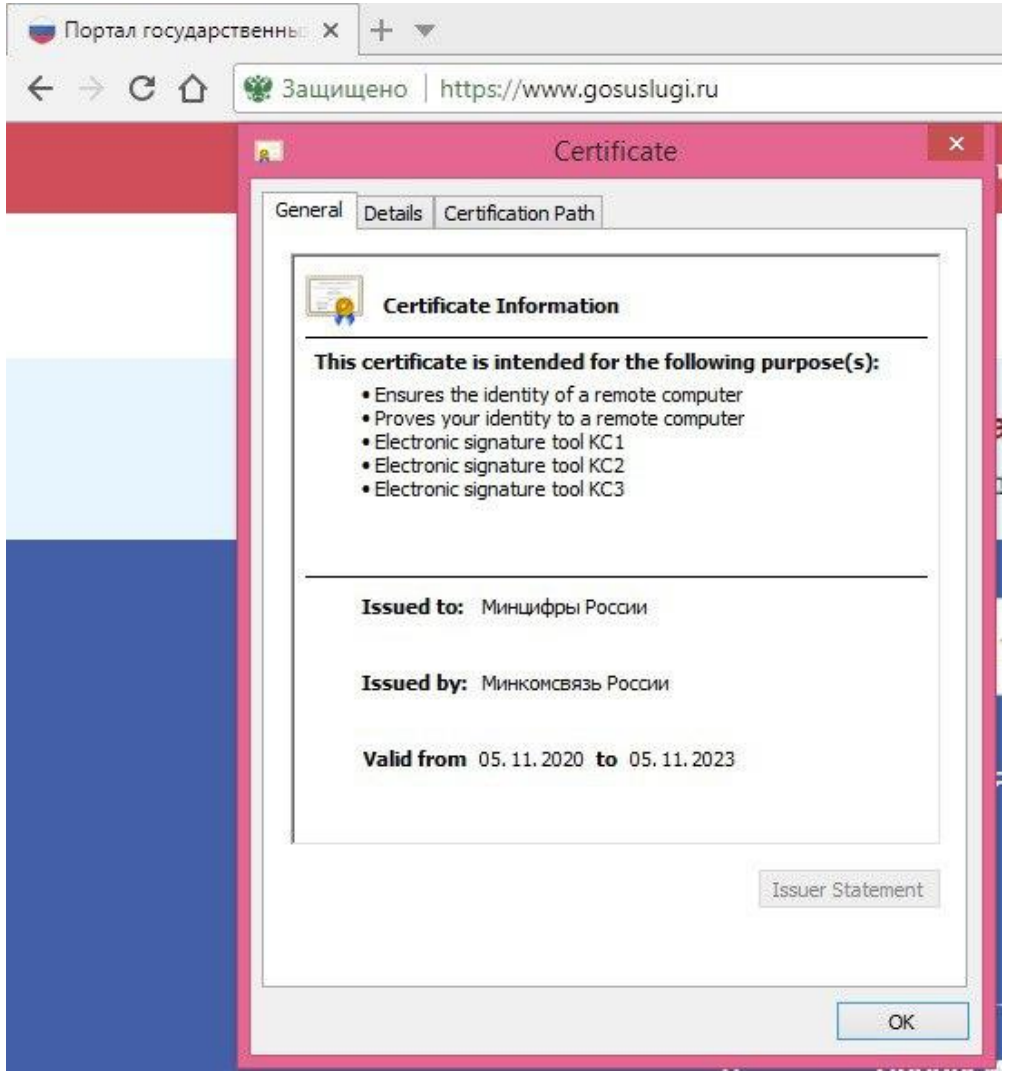
- TLS-сервера с одновременной поддержкой ГОСТ и не ГОСТ
- Браузеры с поддержкой ГОСТ TLS
- Мобильные приложения с поддержкой ГОСТ TLS



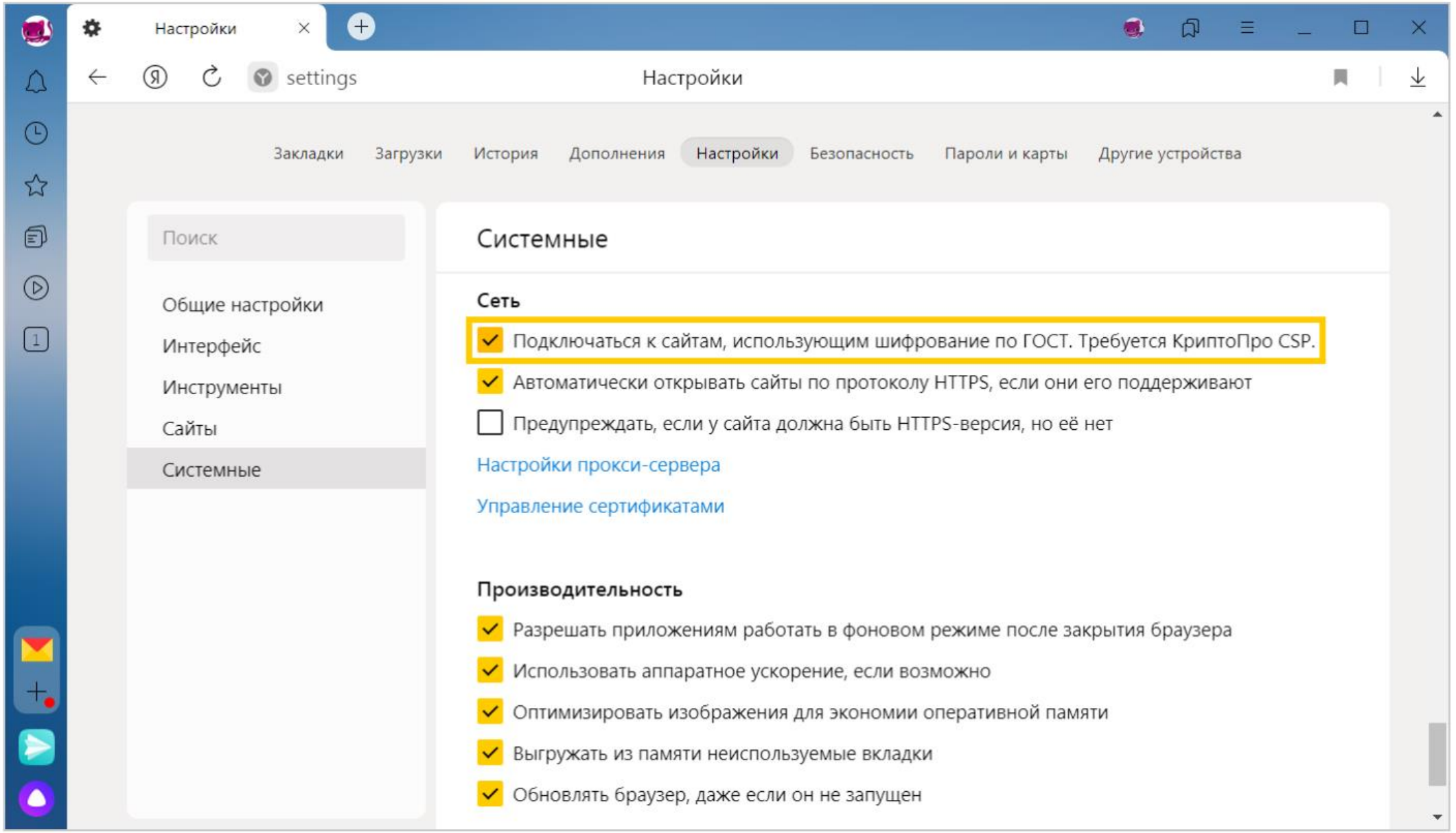
Поддержка ГОСТ TLS на веб-сайтах (примеры)

Защищено

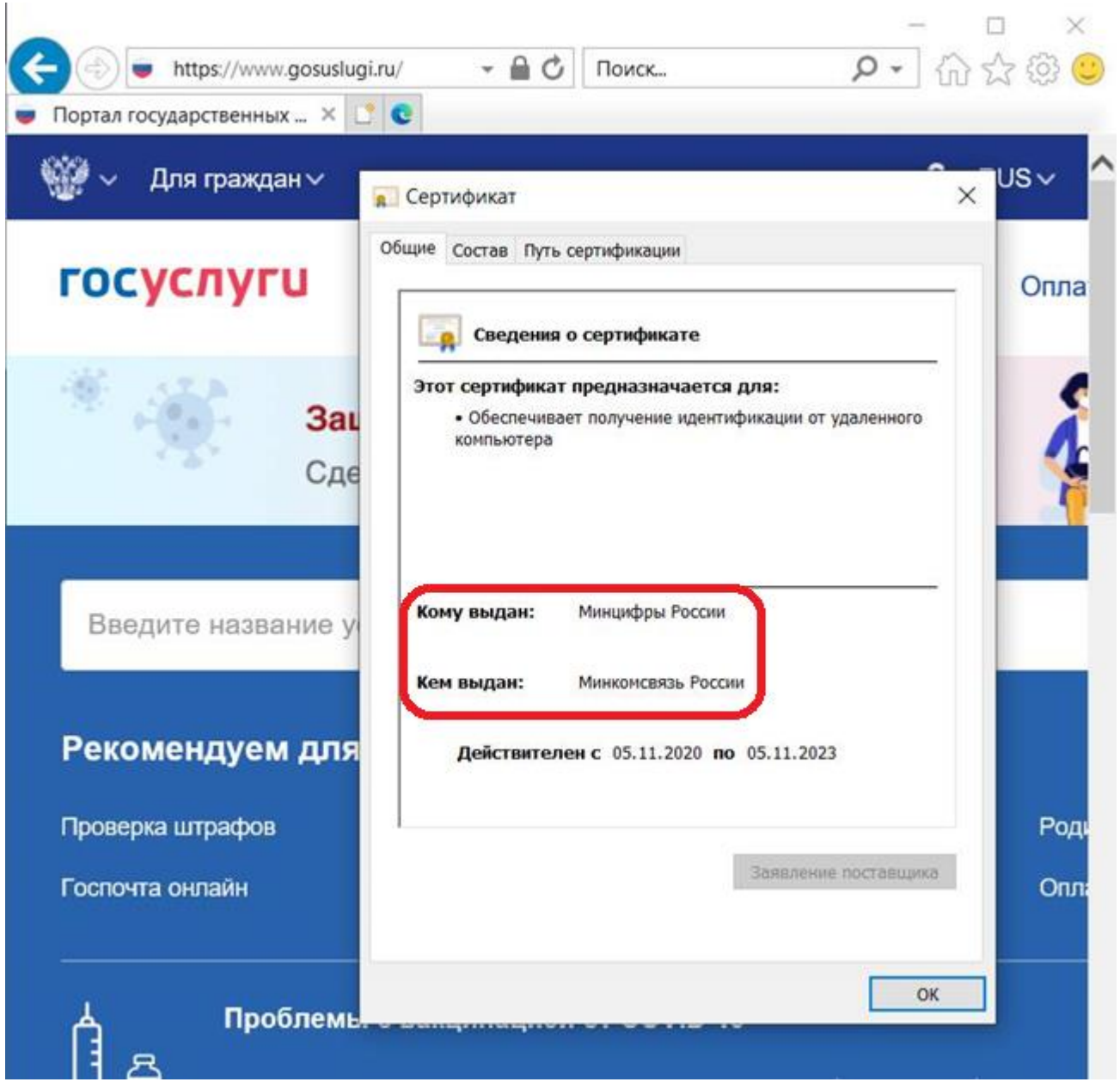
- https://gosuslugi.ru – ЕПГУ
- https://www.mos.ru – госуслуги Москвы
- https://lkul.nalog.ru – личный кабинет налогоплательщика (юрлица)
- https://eruz.zakupki.gov.ru/auth/ – единая ИС в сфере закупок
- https://agregatoreat.ru – единый агрегатор торговли (по 44-ФЗ)
- https://cryptopro.ru – сайт КриптоПро

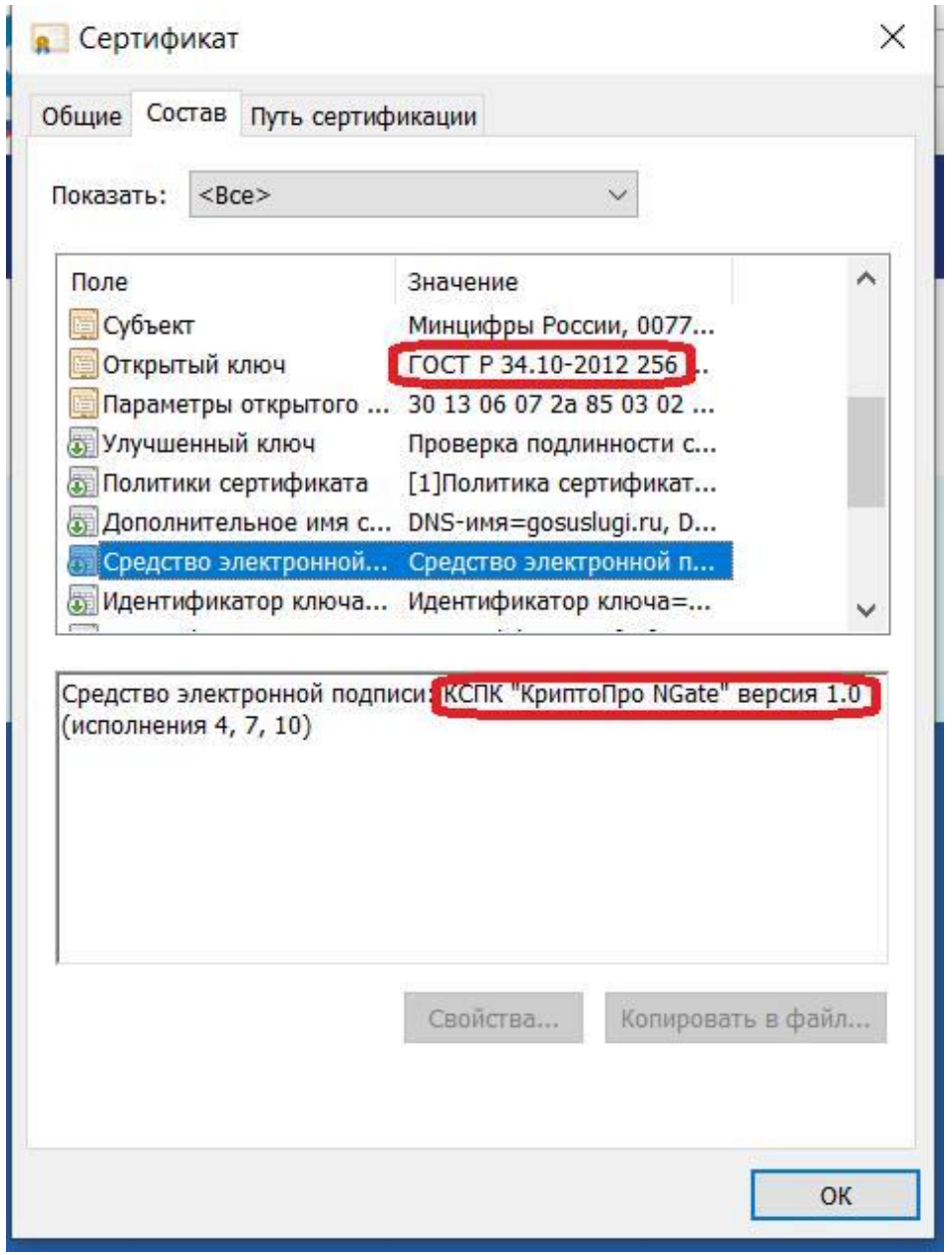


ГОСТ TLS в Яндекс.Браузере включен по умолчанию

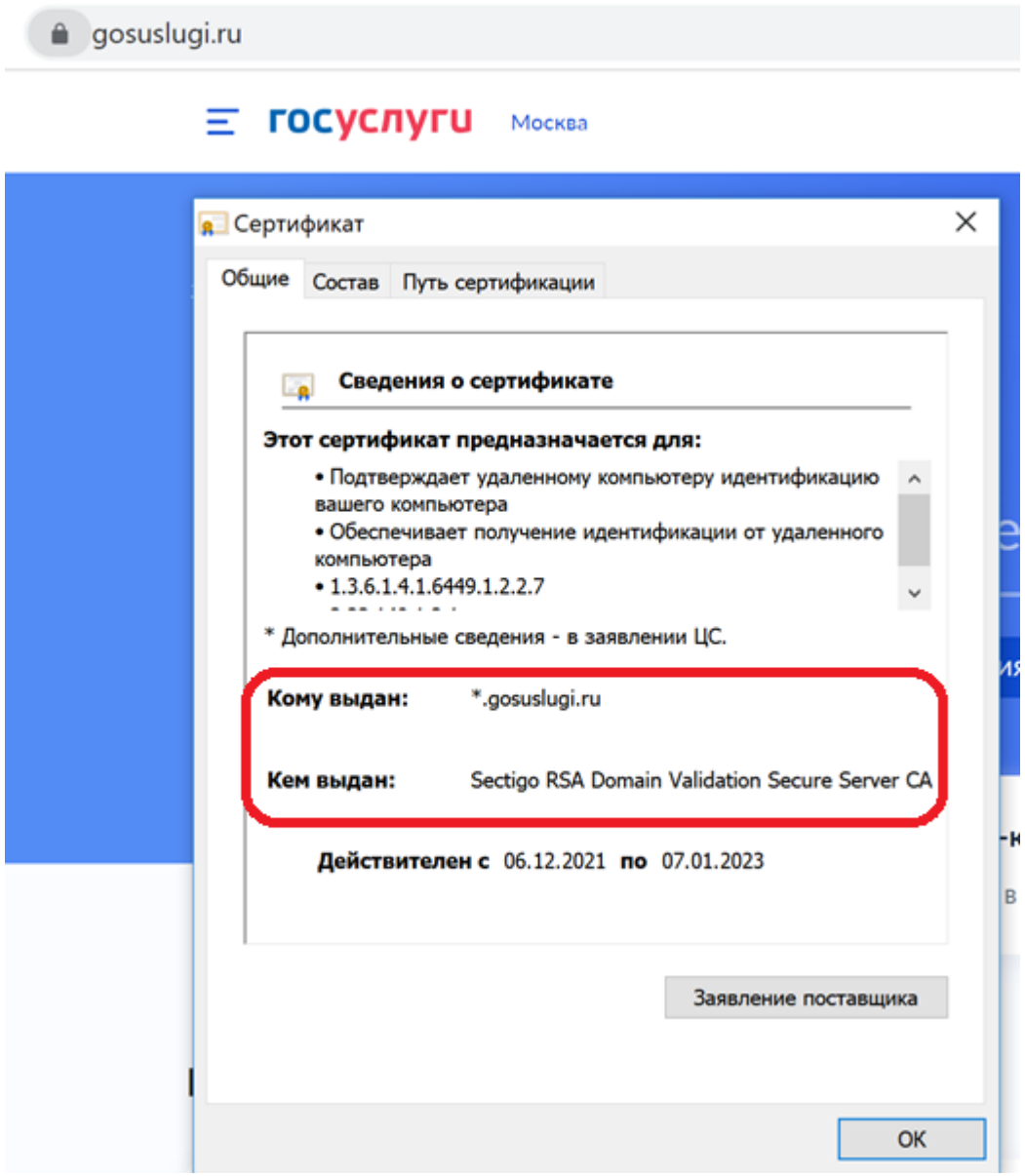


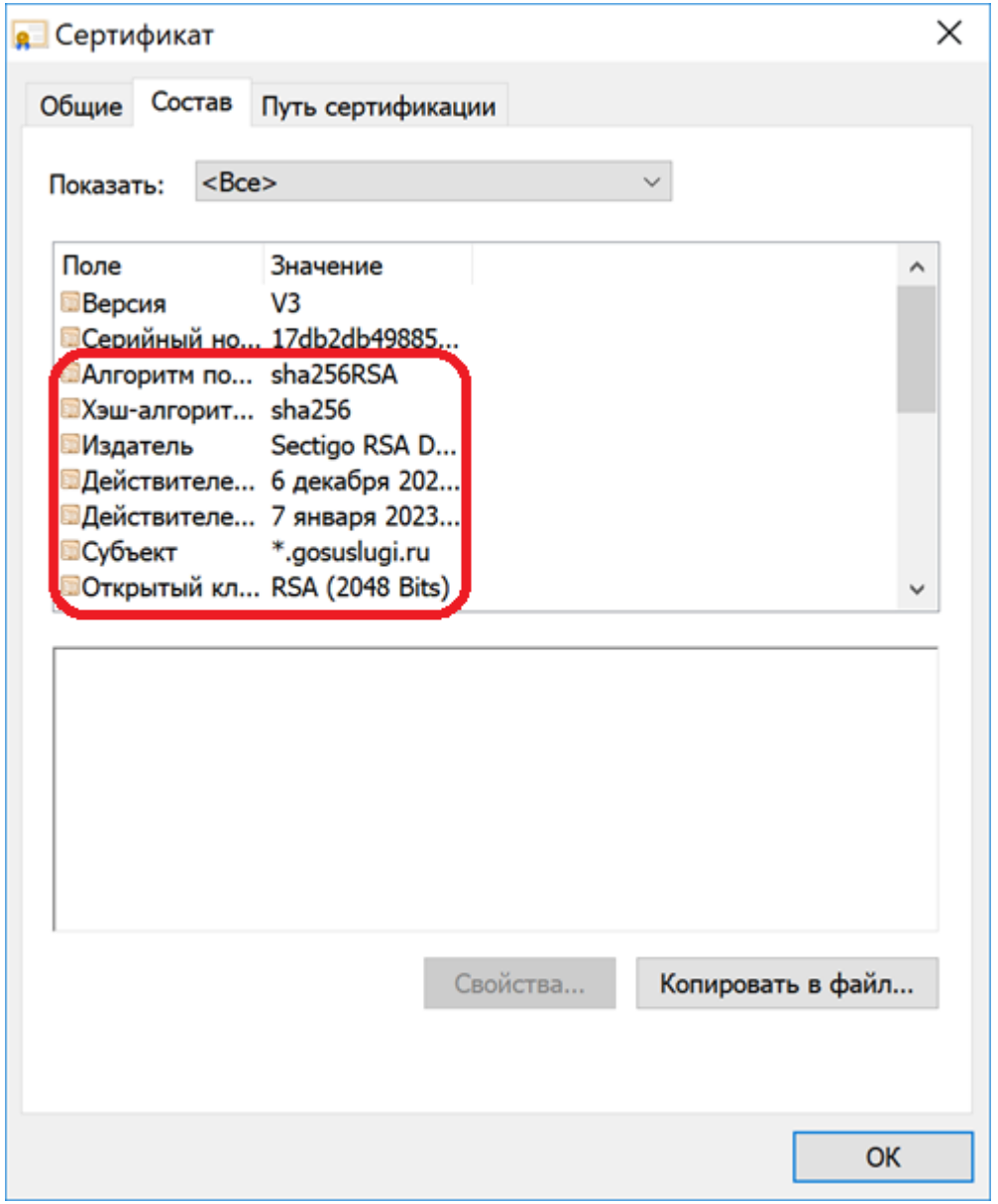
Пример - доступ к ПГУ с браузеров, поддерживающих ГОСТ



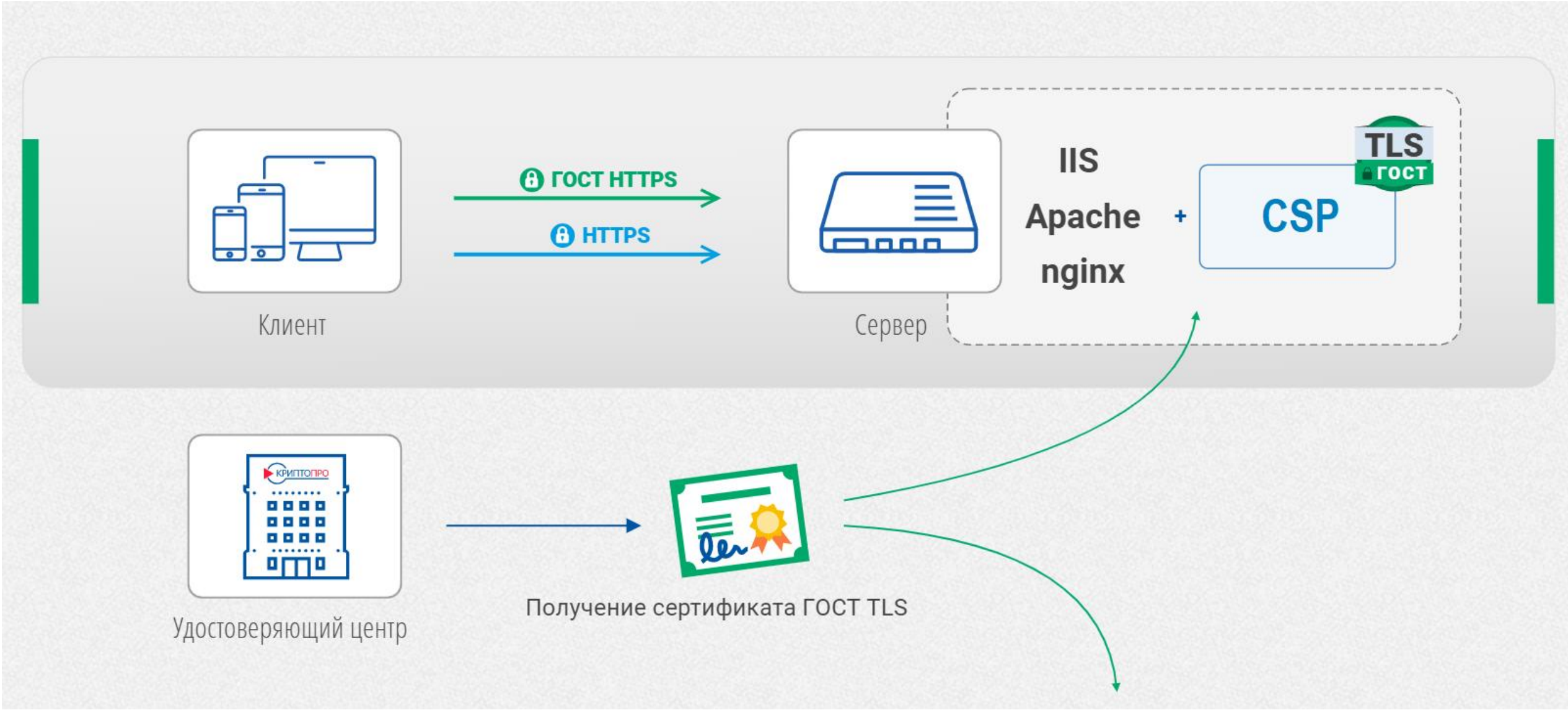


Пример - доступ к ПГУ с браузеров, не поддерживающих ГОСТ

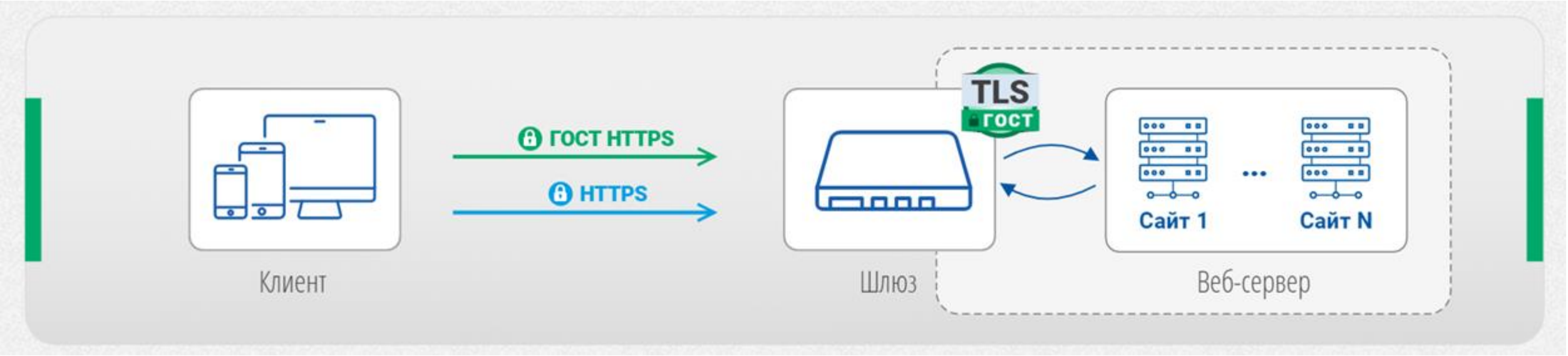




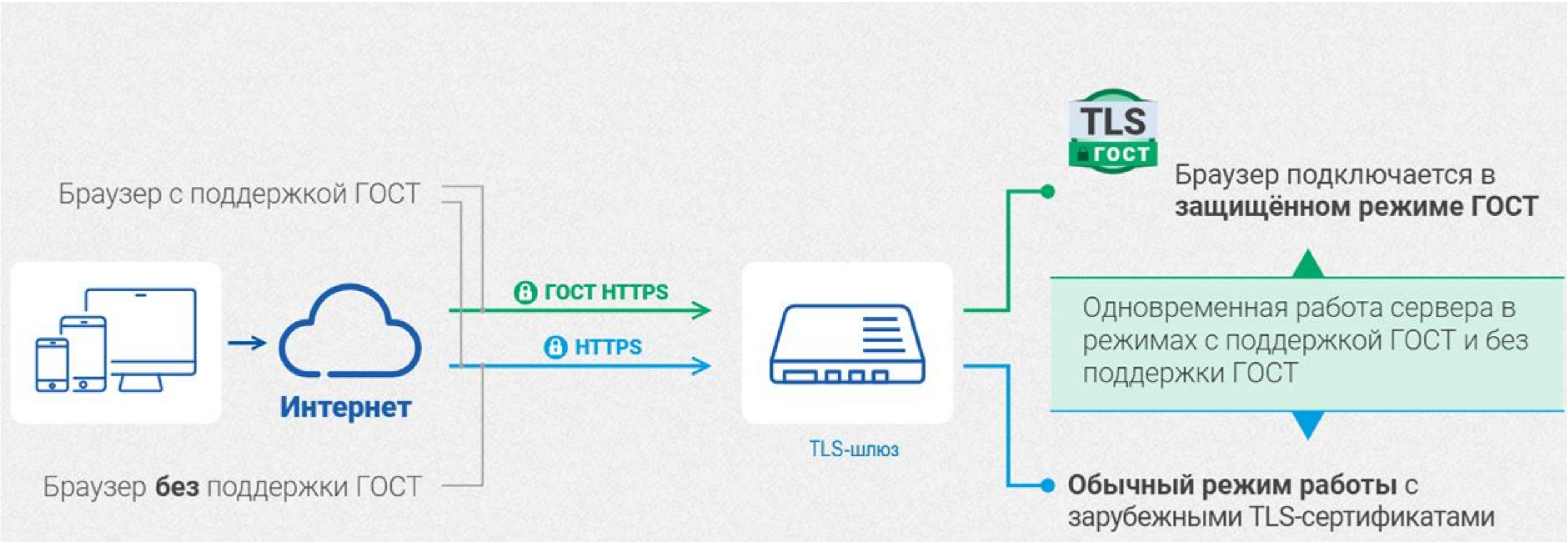
Встраивание ГОСТ при помощи CSP



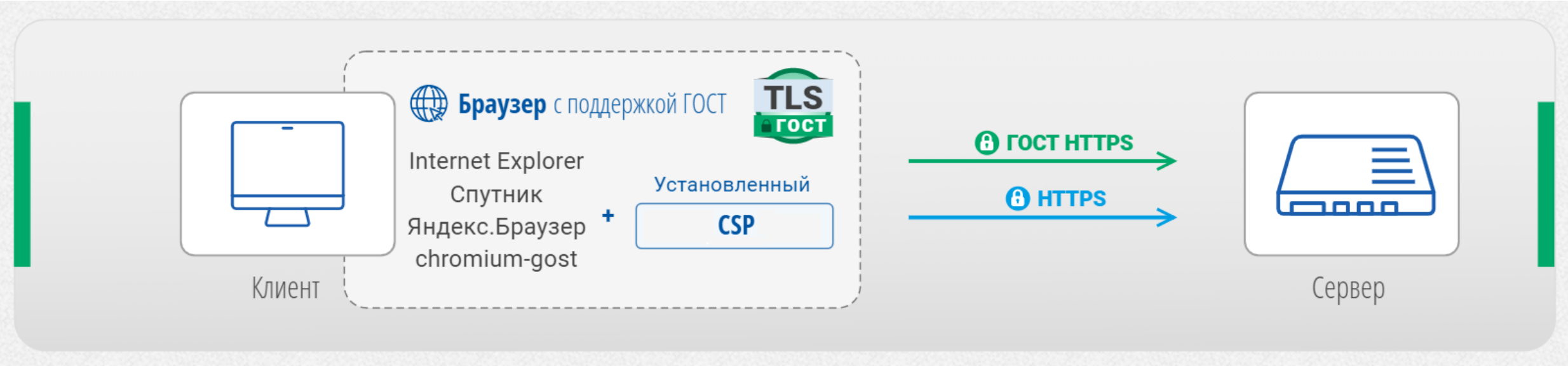
Вынос ГОСТ на отдельную платформу



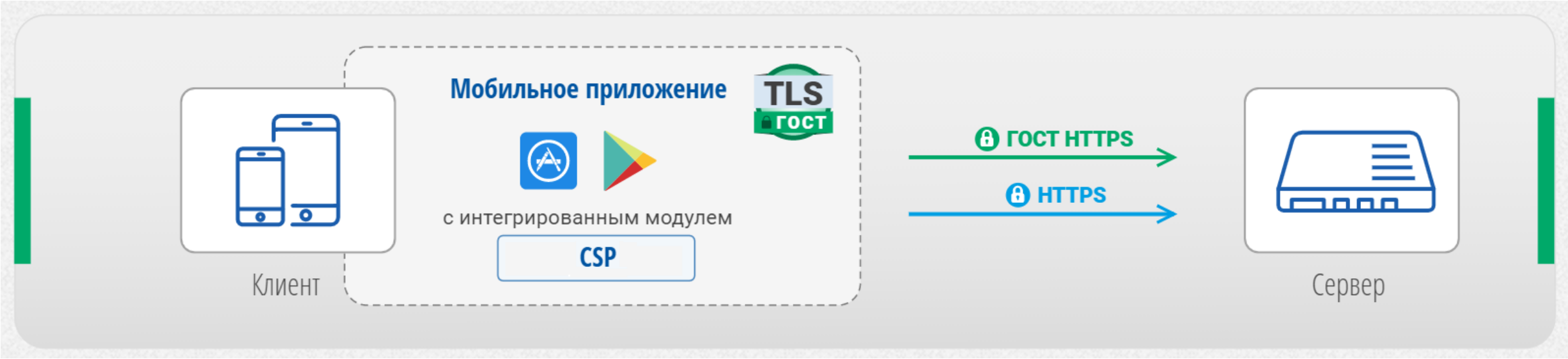
Постепенный переход на ГОСТ TLS



Клиентские решения для стационарных устройств



Клиентские решения для мобильных устройств



КриптоПро CSP 5.0 R2 + nginx/Apache = TLS с ГОСТ

- КриптоПро CSP 5.0 R2 + nginx/Apache (определенных версий) = ГОСТ TLS (без оценки влияния)
- ГОСТ TLS в nginx = применение к исходным текстам специальных патчей из состава КриптоПро CSP 5.0 R2
- ГОСТ TLS в Apache = использование специального бинарного модуля из состава КриптоПро CSP 5.0 R2
- Необходима специальная лицензия КриптоПро CSP для TLS-сервера
- Клиентская лицензия для ПК на КриптоПро CSP не требуется (при одностороннем TLS)

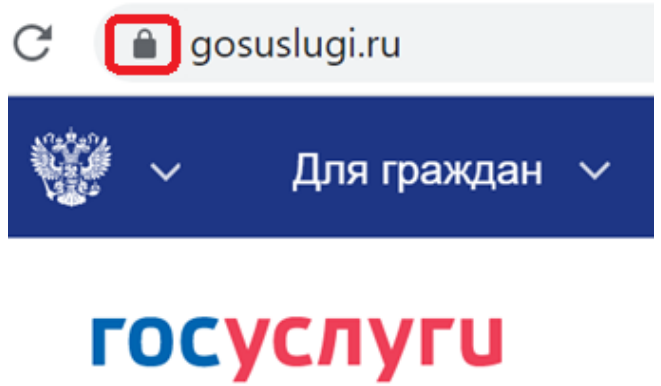
TLS-шлюз КриптоПро NGate

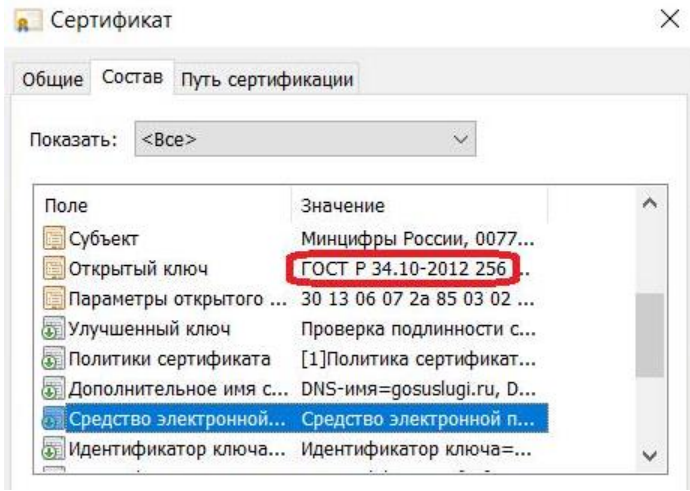
- Наличие сертификатов ФСБ по классам КС1, КС2, КС3
- Одновременная поддержка ГОСТ и не ГОСТ
- Исключение необходимости встраивания криптографии
- Снятие с веб-серверов непрофильной нагрузки
- Клиентская лицензия для ПК на КриптоПро CSP не требуется (при одностороннем TLS)
- Высокая производительность (до 45 000 одновременных соединений)
- Возможность интеграции с Web Application Firewall
- Поддержка виртуализации

NG КРИПТОПРО NGate TLS-VPN

Тестирование работы ГОСТ TLS на стороне пользователя

1. Установите один из браузеров, поддерживающих ГОСТ TLS, например, Яндекс.Браузер
2. Установите российский криптопровайдер (например, КриптоПро CSP)
3. Установите корневой сертификат УЦ (при использовании CryptoPro TLS CA сертификат устанавливается автоматически при установке КриптоПро CSP)
4. Для примера перейдите на сайт, поддерживающий ГОСТ, например, https://gosuslugi.ru
5. Откройте сертификат сервера (щелкнув по замку)
6. Убедитесь, что сертификат поддерживает ГОСТ. Соединение с сайтом по ГОСТ TLS установлено.
7. Теперь вы будете заходить по протоколу ГОСТ TLS на все поддерживающие его сайты.
8. Остальные сайты, как и раньше, будут доступны по обычному TLS





Полезные ресурсы по TLS

- Группа в Telegram, посвященная НУЦ Russian Trusted Root CA: https://t.me/RussianTLS
- Варианты реализации TLS с ГОСТ: https://cryptopro.ru/products/csp/tls
- TLS с ГОСТ на nginx/Apache: https://cryptopro.ru/products/csp/tls/gost-nginx-apache
- Статья Яндекса про поддержку сайтов с национальными сертификатами в Я.Браузере: https://habr.com/ru/company/yandex/blog/655185/
- Тематические групп в Telegram по УЦ и ЭП
- Группа в Telegram по NGate: https://t.me/cpngate
- Дистрибутивы на КриптоПро CSP и NGate со встроенной лицензий на три месяца: https://cryptopro.ru/downloads

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Общие вопросы: **info@cryptopro.ru**
Контрактный отдел: **kpo@cryptopro.ru**
Для дилеров: **dealer@cryptopro.ru**