КРИПТОПРО

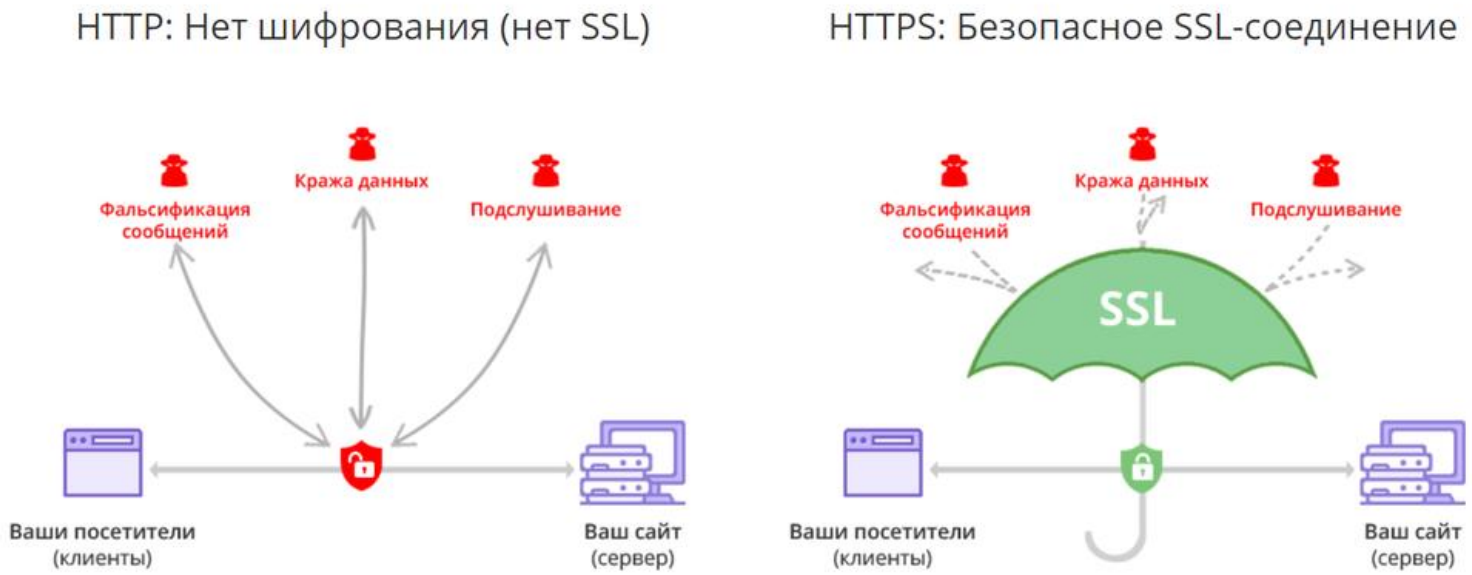
Ключевое слово
в защите информации

Защита доступа к веб-сайтам и корпоративным ресурсам в условиях санкций

Павел Луцик, Директор по развитию бизнеса и работе с партнерами

21 апреля 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:

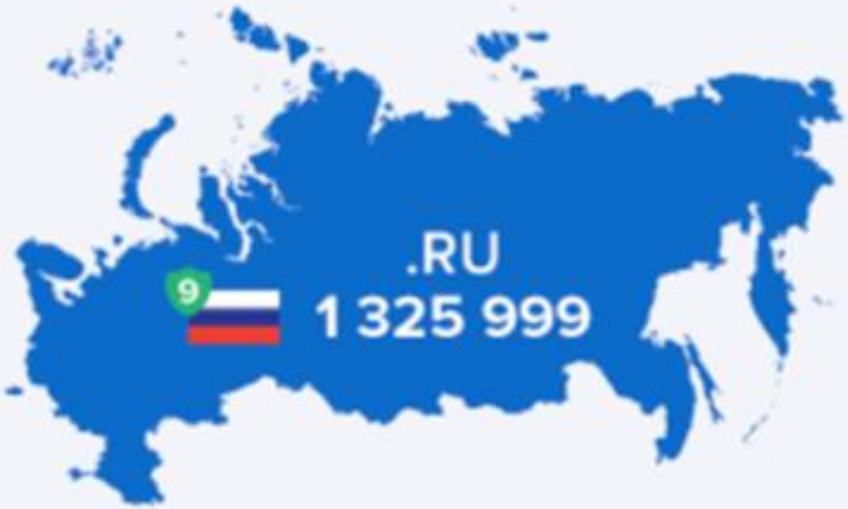
- Фишинга (посещения поддельных сайтов)
- Внесения несанкционированных изменений в передаваемые данные
- Кражи передаваемой информации

Персональный сертификат не является обязательным для TLS и:

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

ТОП-10 стран по количеству используемых TLS-сертификатов

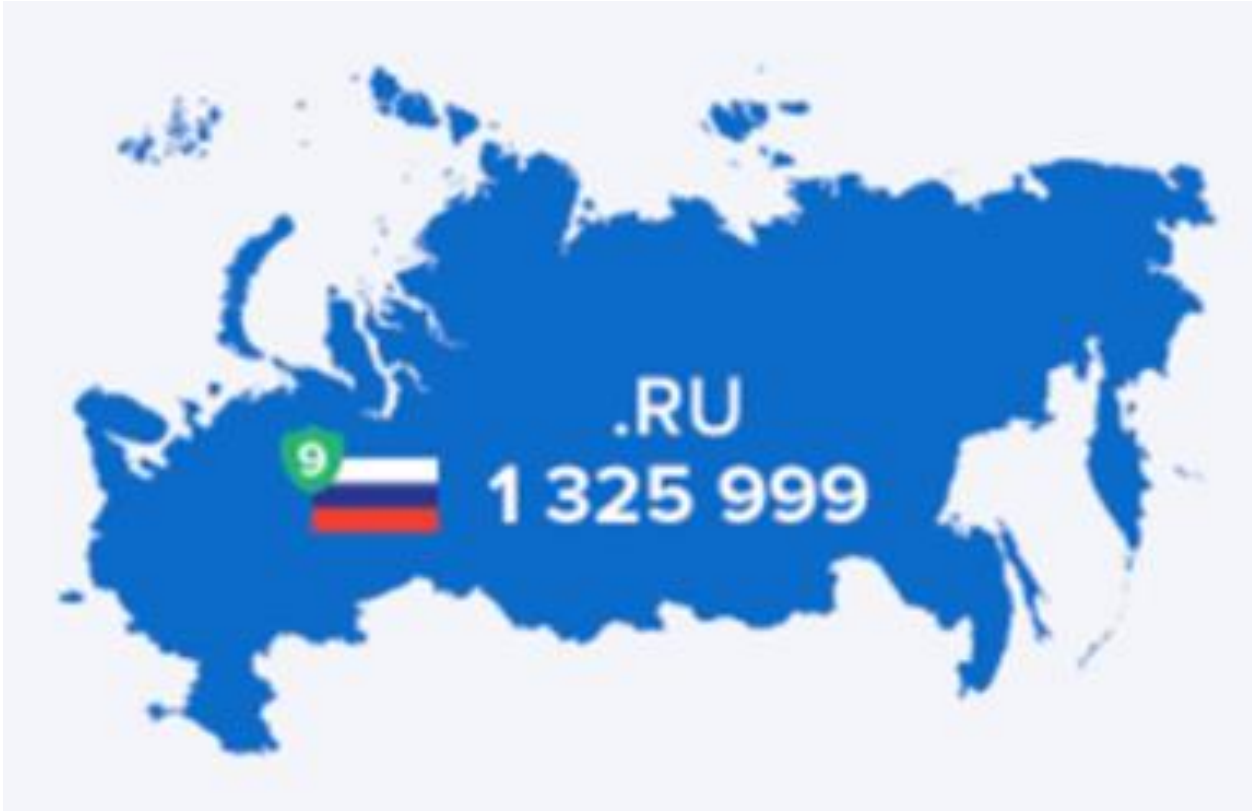
1. .US 45 619 376
2. .DE 6 841 157
3. .JP 2 410 826
4. .UK 2 397 158
5. .NL 2 215 705
6. .FR 2 058 494
7. .DK 1 607 158
8. .CA 1 407 358
9. .RU 1 325 999
10. .CN 1 115 118



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

Основной риск:

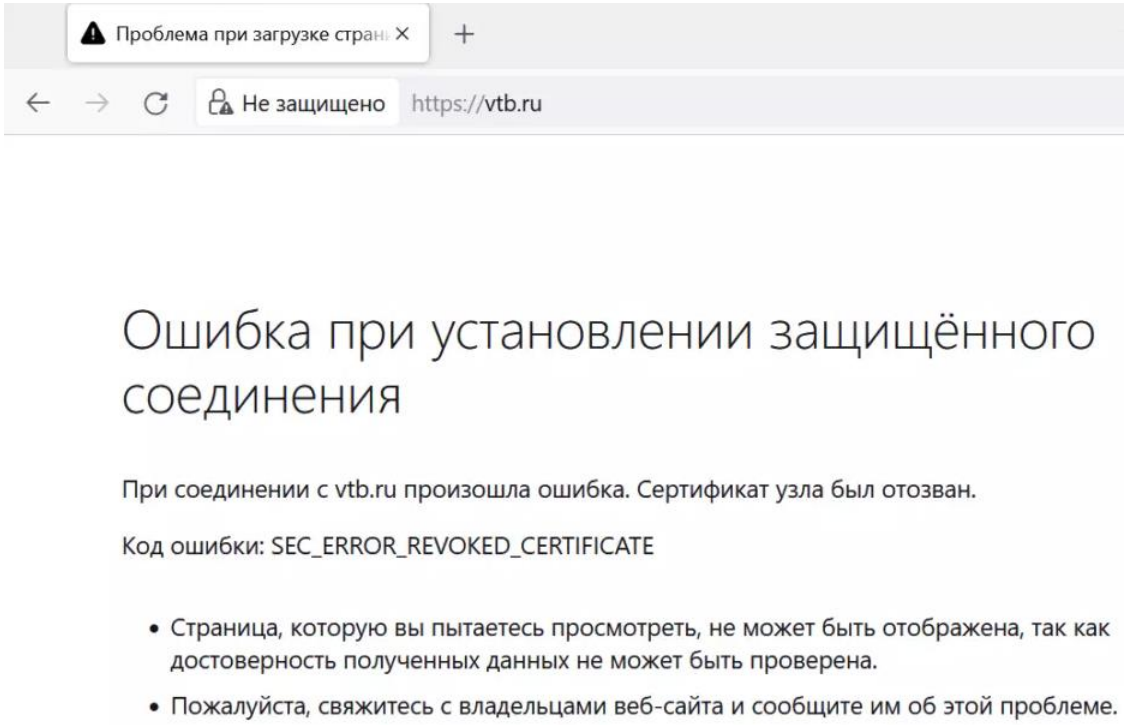
- Отзыв действующего сертификата

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

- 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



Временный вариант – TLS-сертификат лояльного 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

Текущая схема НУЦ для выпуска RSA TLS-сетификатов

НУЦ

Root CA
RSA

Sub CA
RSA

Минцифры

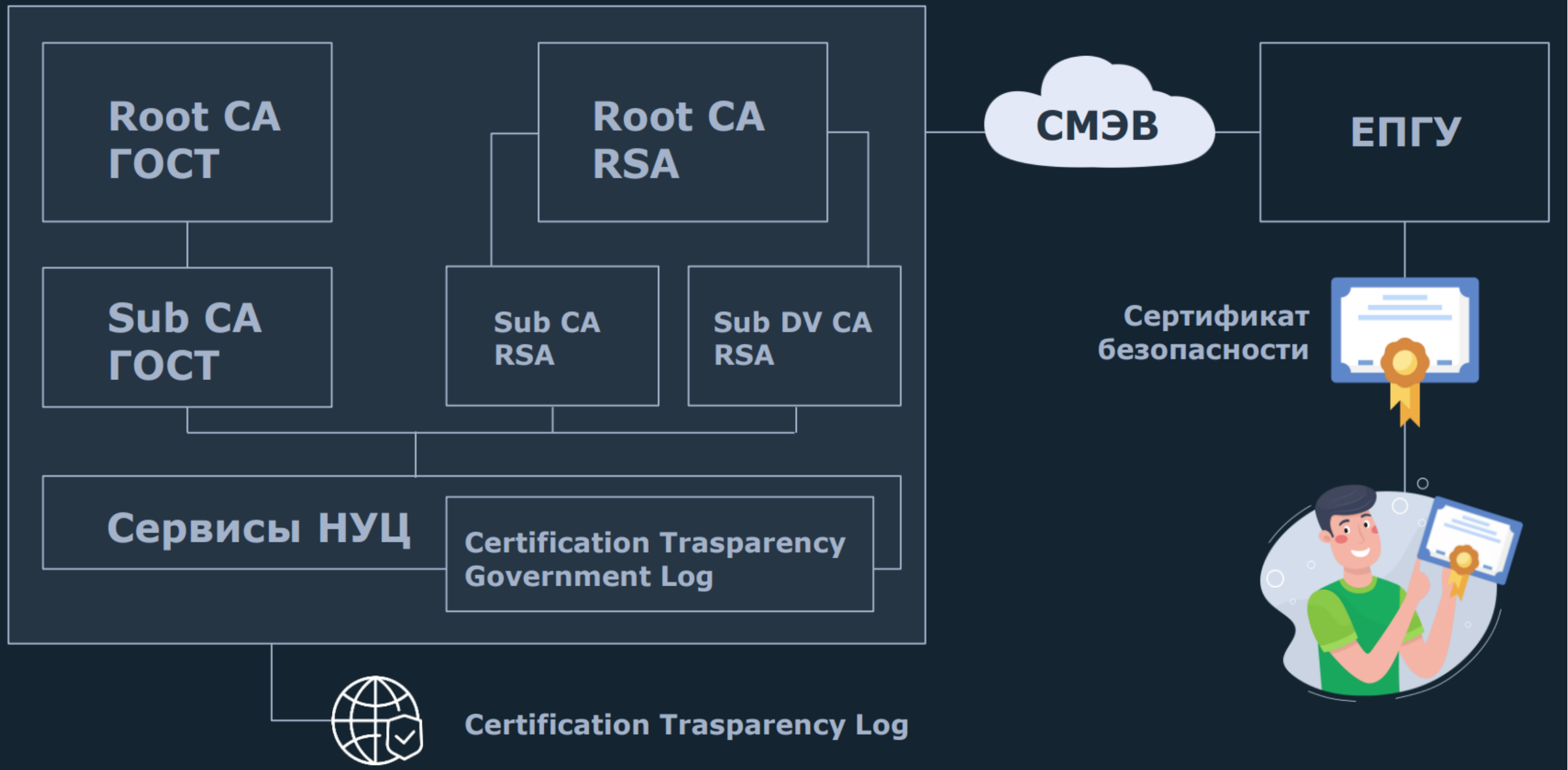
ЕПГУ

Сертификат
безопасности

Доверие к сертификатам в браузерах

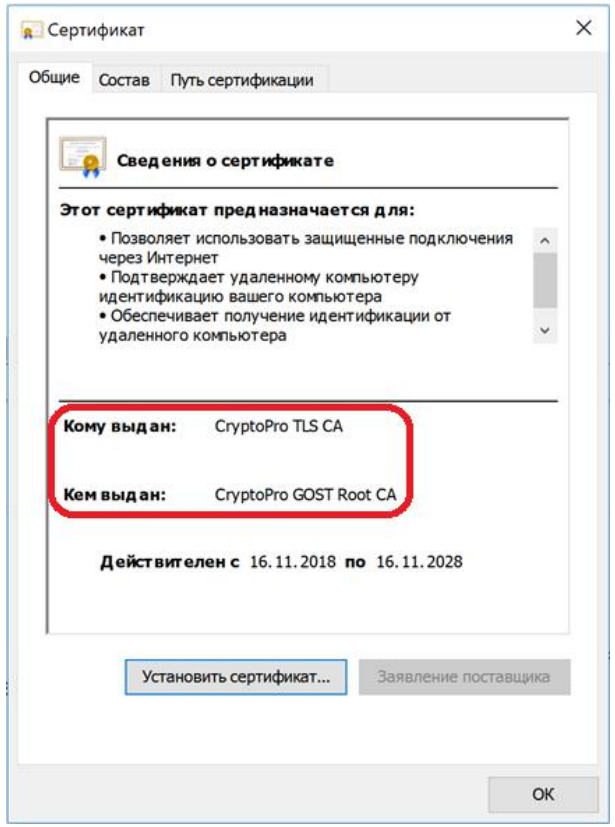
- В браузеры Яндекс и Атом добавлен корневой RSA-сертификат Минцифры
- Я.Браузер признает сертификаты НУЦ только для доменов из списка на сайте: www.gosuslugi.ru/tls
- Если посещаемого сайта нет в этом списке, отобразится стандартная ошибка и браузер не даст посетить сайт

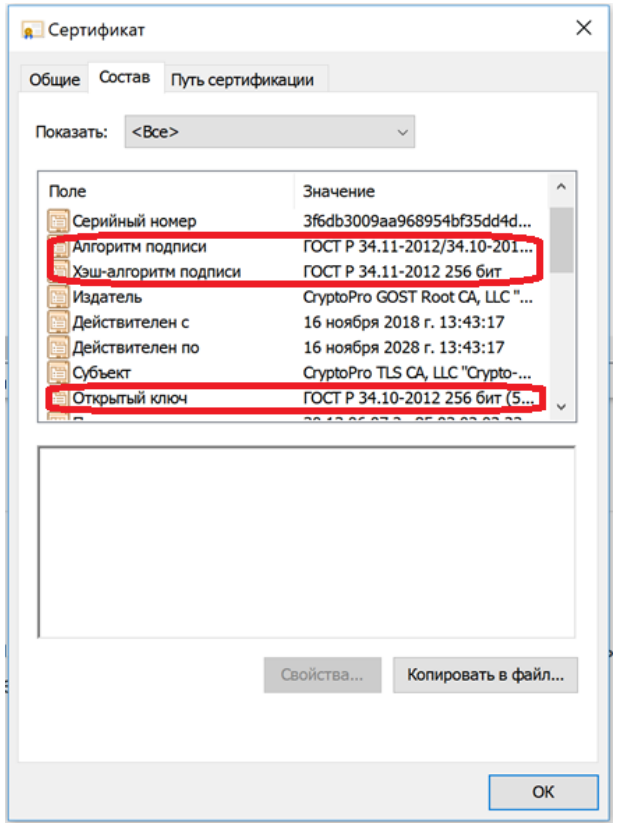
Целевая схема НУЦ для выпуска RSA и ГОСТ TLS-сертификаты



Рекомендуемый 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





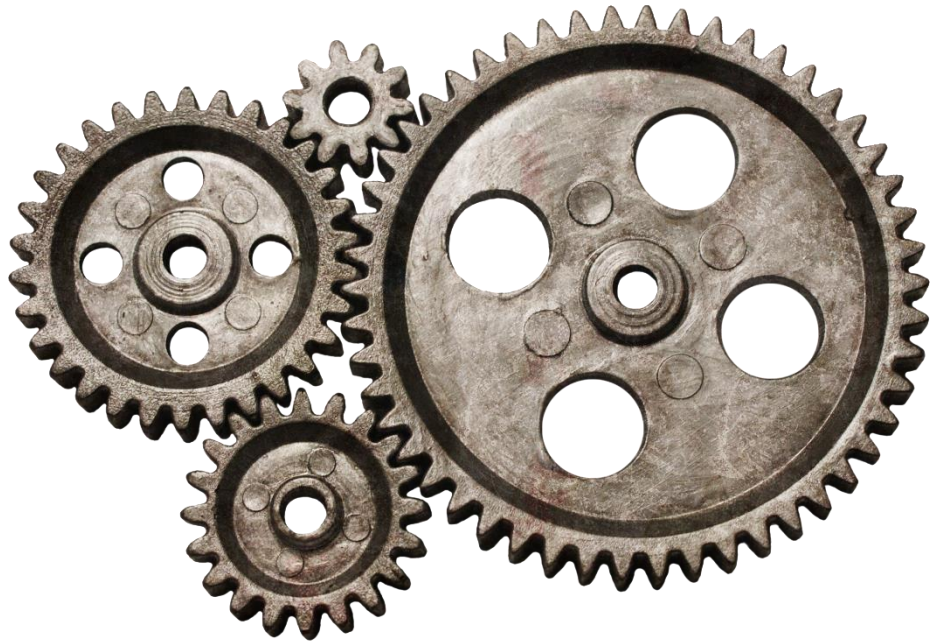
Доверие к корневым сертификатам в КриптоПро CSP

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

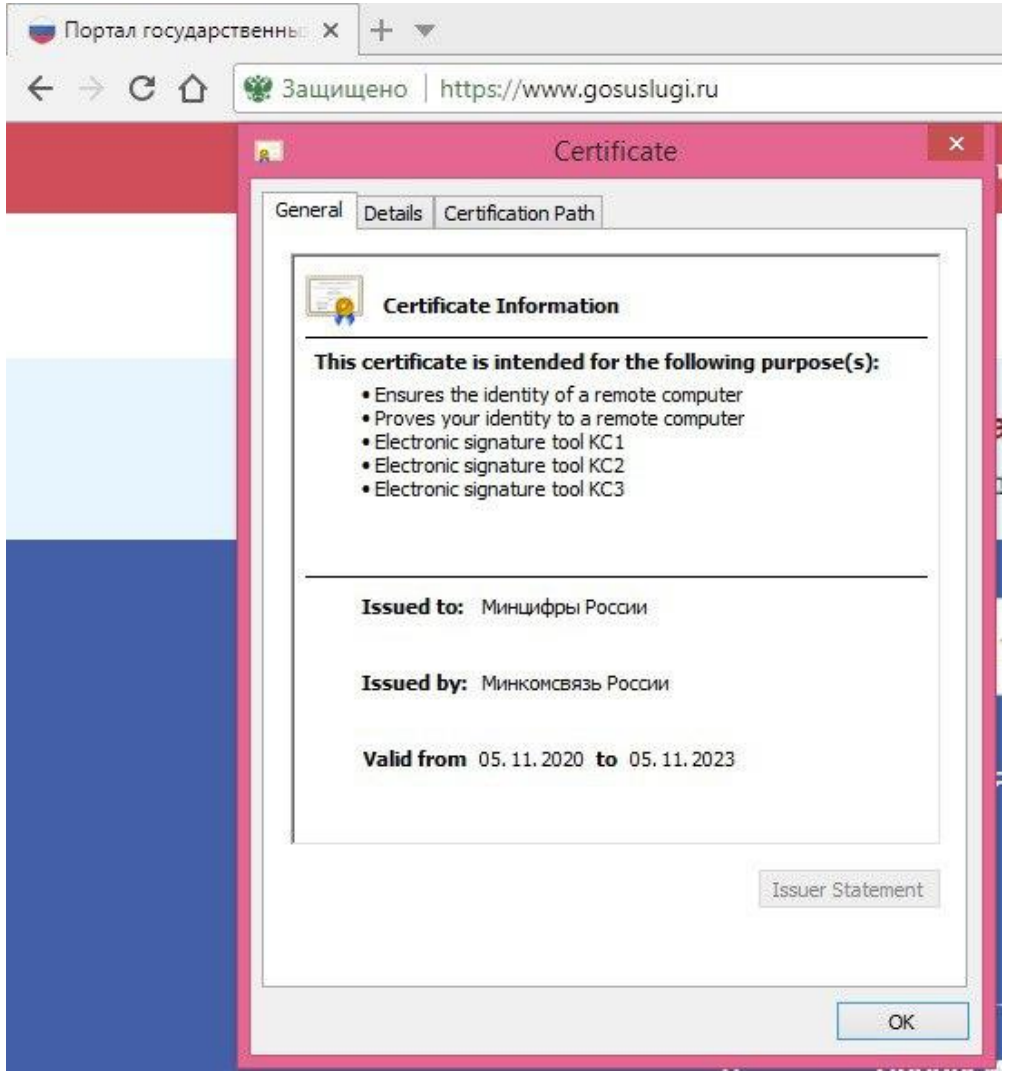
- TLS-сервера с одновременной поддержкой ГОСТ и не ГОСТ
- Браузеры с поддержкой ГОСТ TLS
- Мобильные приложения с поддержкой ГОСТ TLS



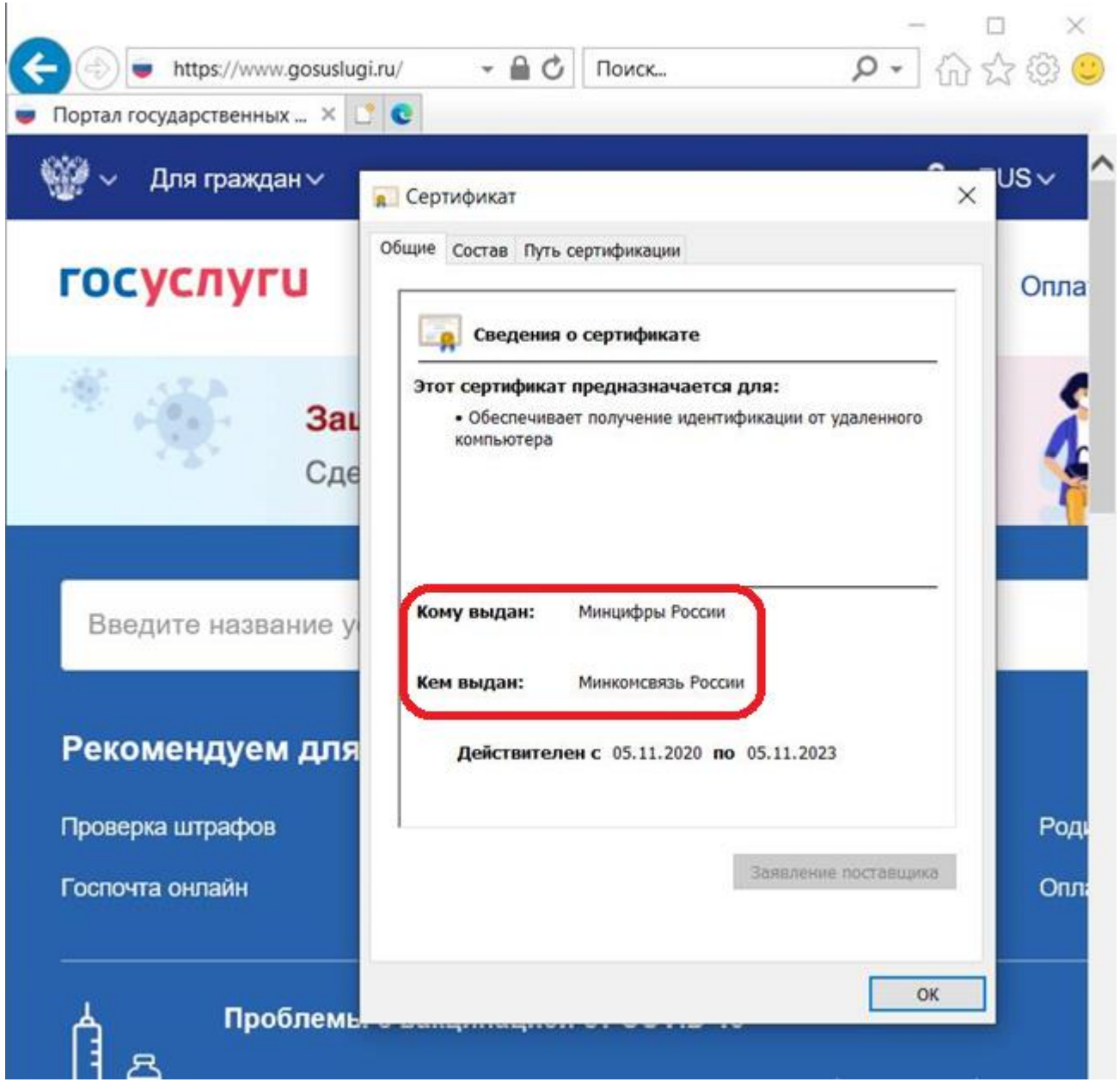
Поддержка ГОСТ TLS на веб-сайтах (примеры)

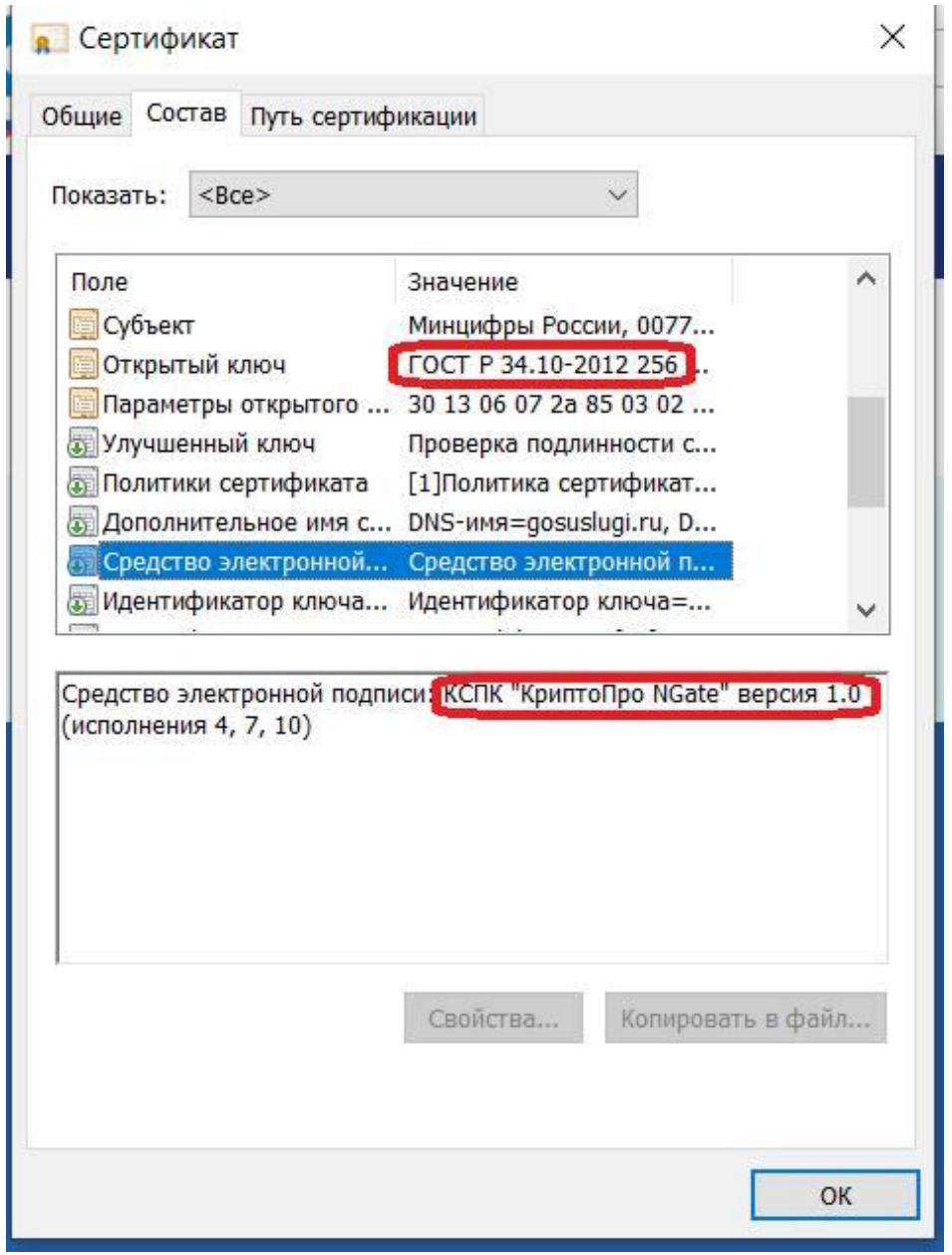
Защищено

- 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

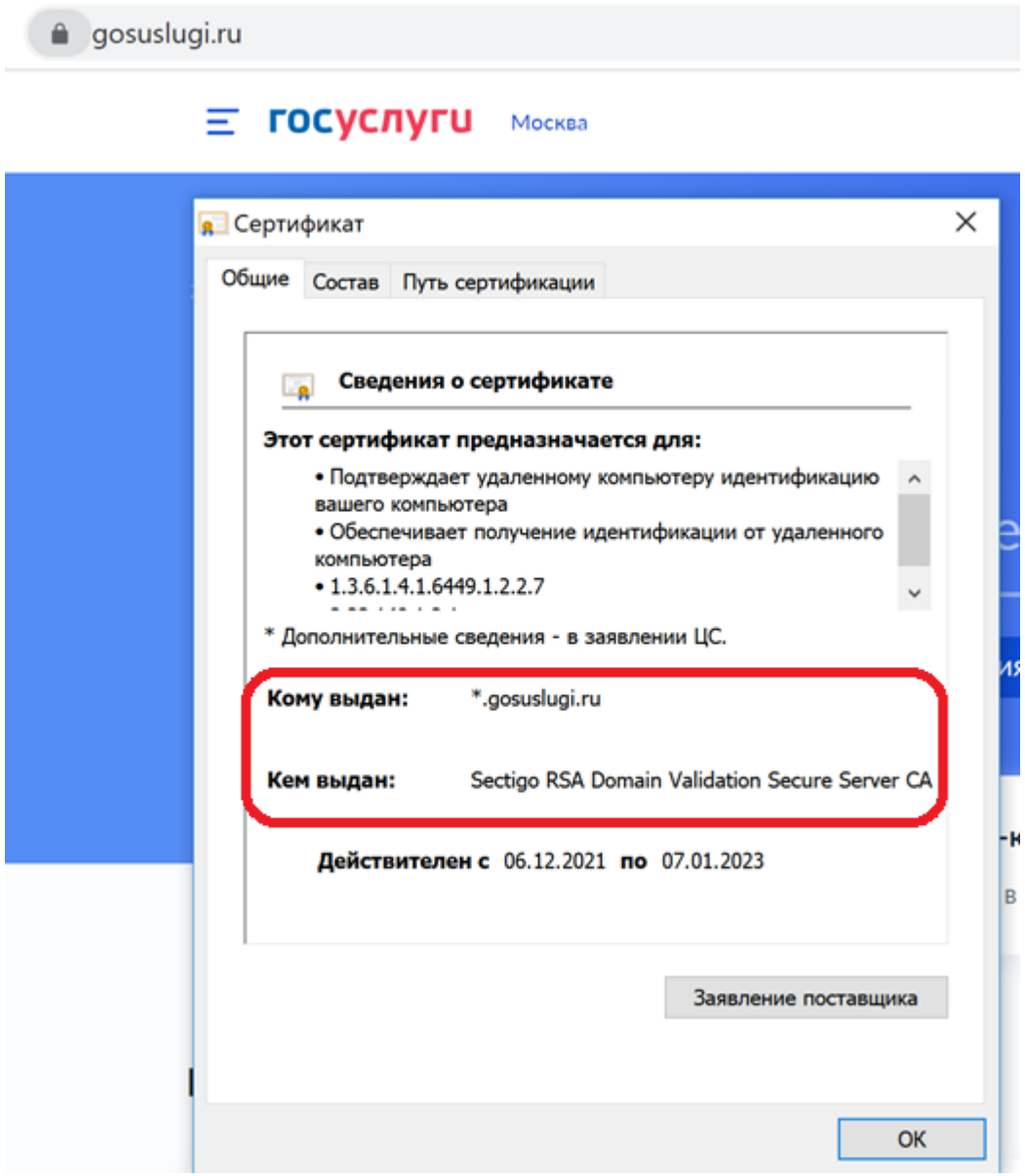


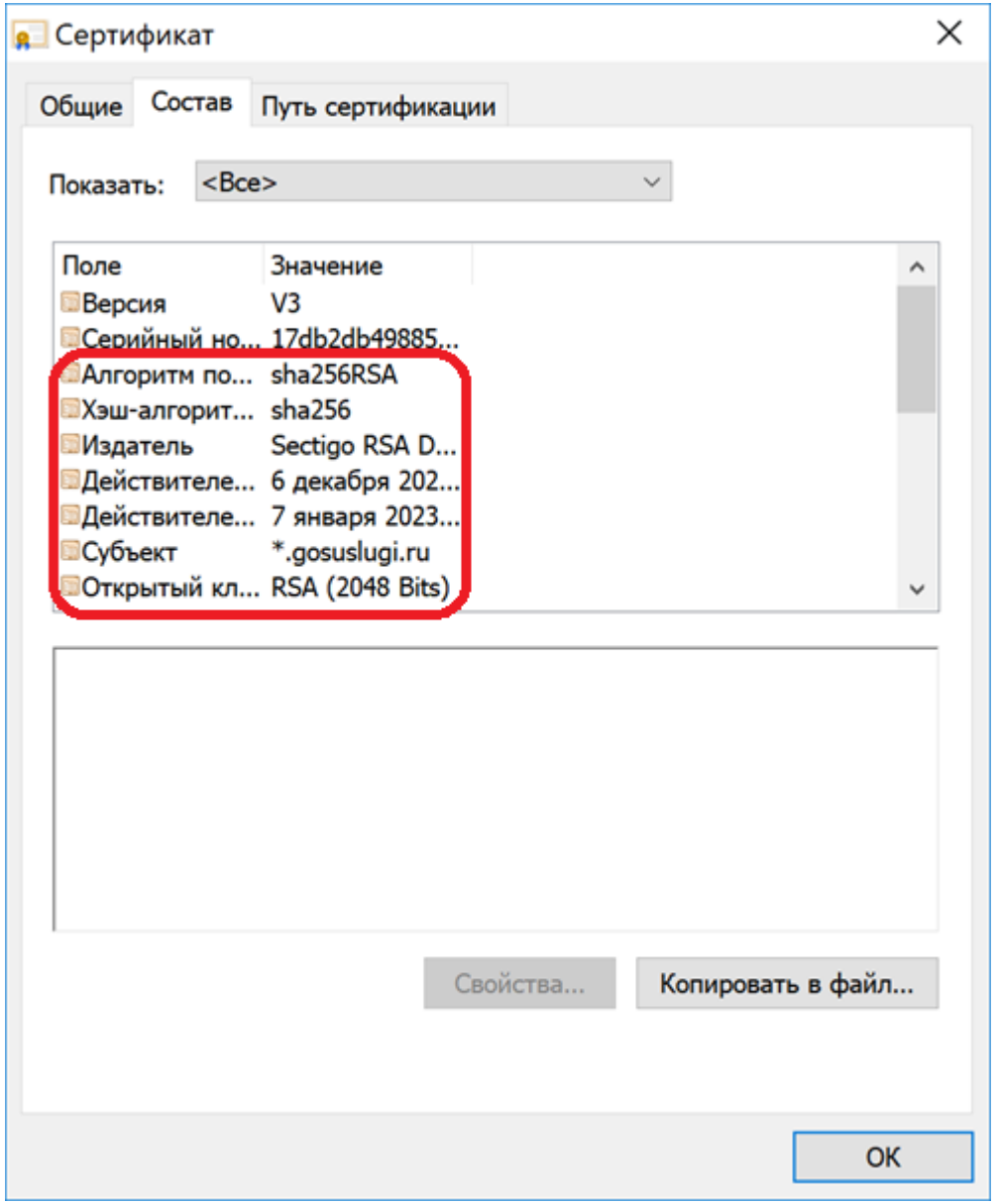
Пример - доступ к ПГУ с браузеров, поддерживающих ГОСТ



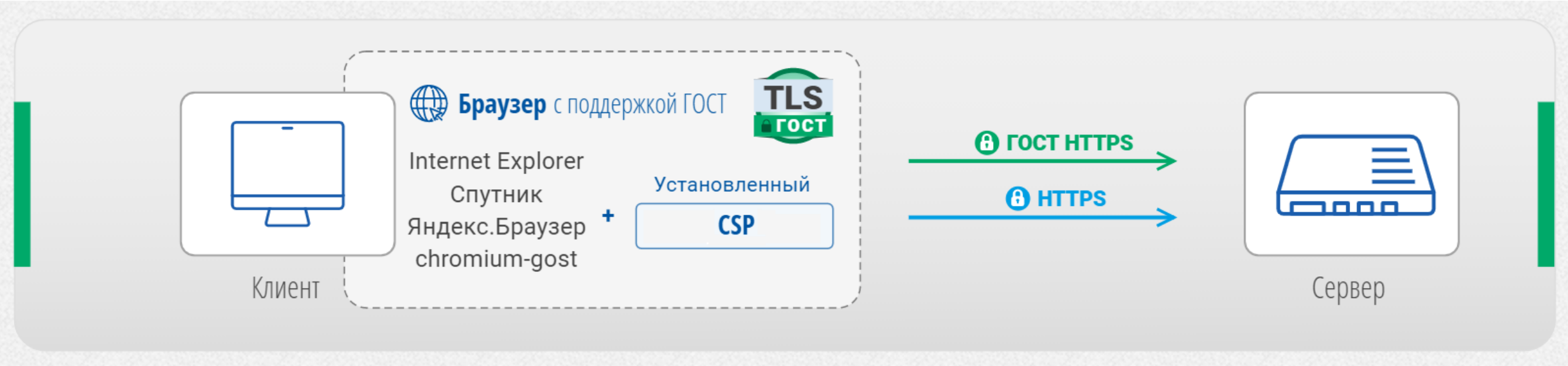


Пример - доступ к ПГУ с браузеров, не поддерживающих ГОСТ

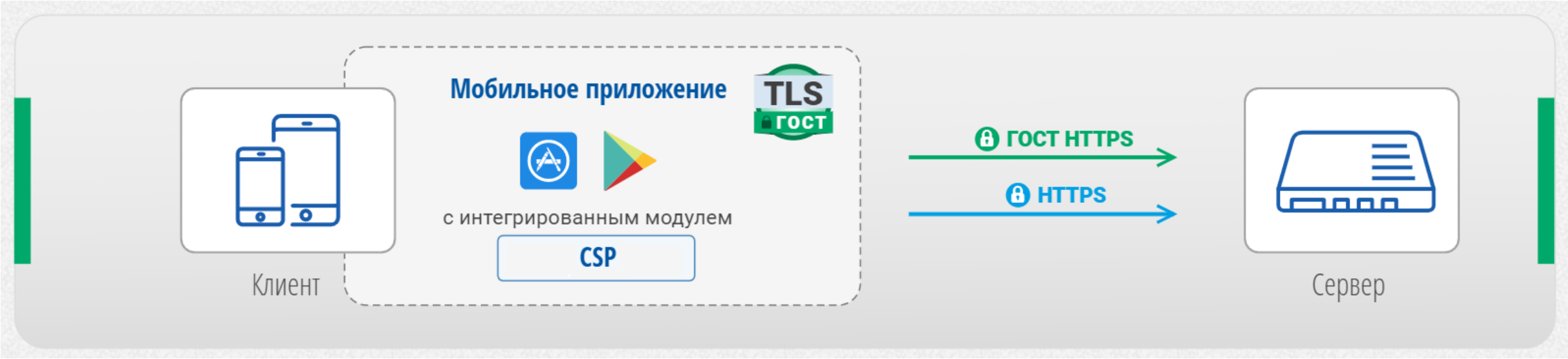




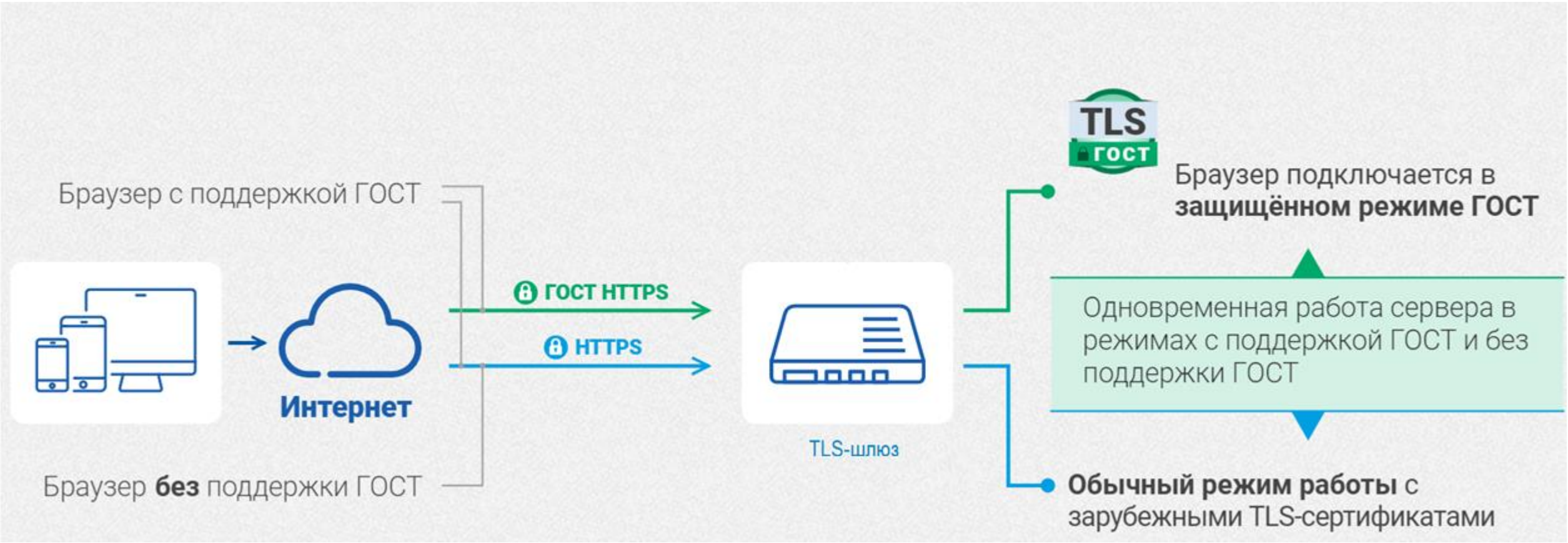
Клиентские решения для стационарных устройств



Клиентские решения для мобильных устройств

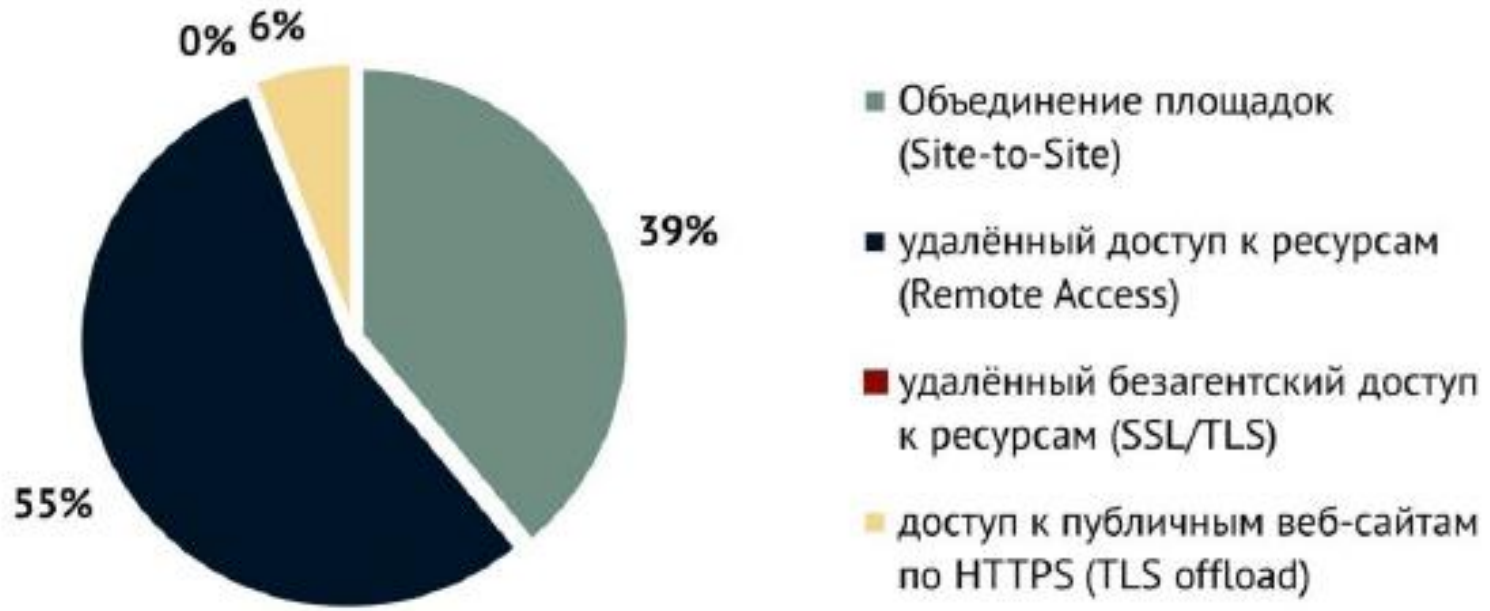


Постепенный переход на ГОСТ TLS при веб-доступе



VPN-доступ к произвольным корпоративным ресурсам

Для каких сценариев вы ищите замену зарубежных VPN-шлюзов?



Универсальный TLS-шлюз и VPN КриптоПро NGate

NG КРИПТОПРО NGate TLS-VPN

Преимущества NGate

- Сертификаты ФСБ по классам КС1, КС2, КС3
- Бесплатный VPN-клиент
- Клиентская лицензия на КриптоПро CSP зачастую не требуется
- Одновременная поддержка ГОСТ и не ГОСТ
- Поддержка виртуализации и всех современных ОС
- Исключение необходимости встраивания криптографии
- Снятие с веб-серверов непрофильной нагрузки
- Высокая производительность

Преимущества NGate

- Поддержка протоколов TLS и IPSec
- Четыре режима работы:
  - Доступ к публичным веб-сайтам (TLS Offload)
  - Портальный доступ к веб-ресурсам (Web Portal)
  - Удаленный доступ к произвольным ресурсам (Remote Access)
  - Объединение площадок в единую сеть VPN (Site-to-Site)
- Поддержка различных видов аутентификации и MFA
  - Без аутентификации (прозрачно)
  - Логин/пароль (MS AD/LDAP)
  - Сертификат
  - OTP через Radius

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**