КРИПТОПРО

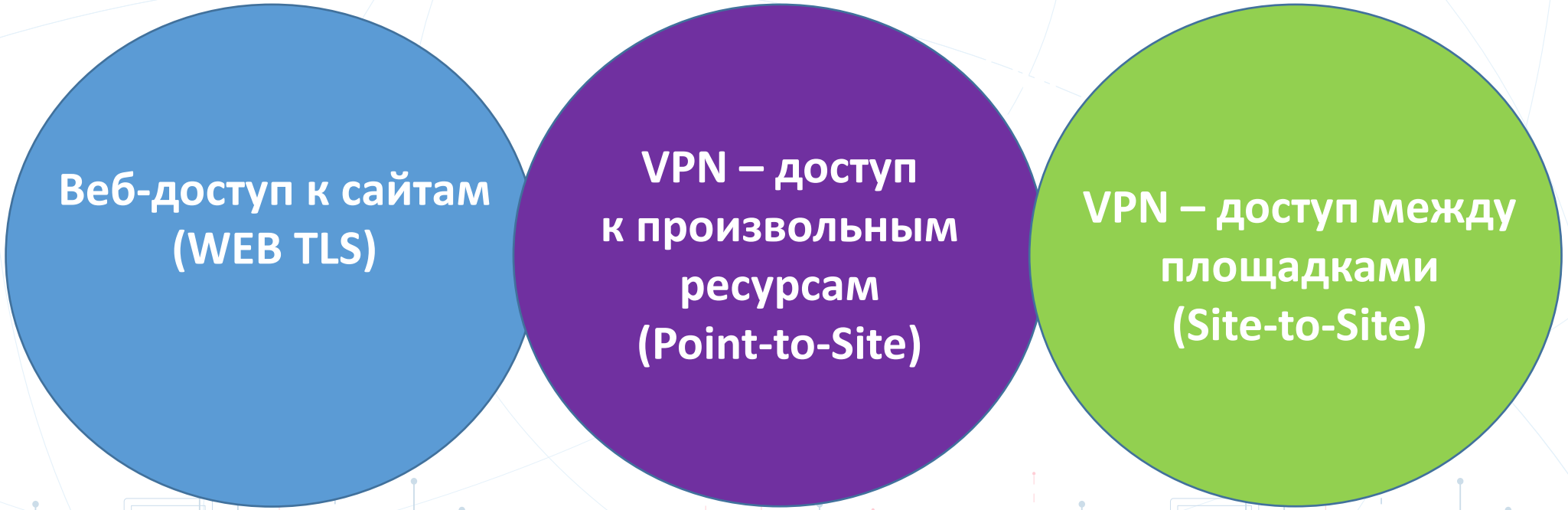
Ключевое слово
в защите информации

Как обеспечить защищенный доступ к веб-сайтам и корпоративным ресурсам в условиях санкций и ухода с российского рынка иностранных ИБ-производителей

Павел Луцик, Директор по развитию бизнеса и работе с партнерами

15 сентября 2022 года

Три основных типа доступа



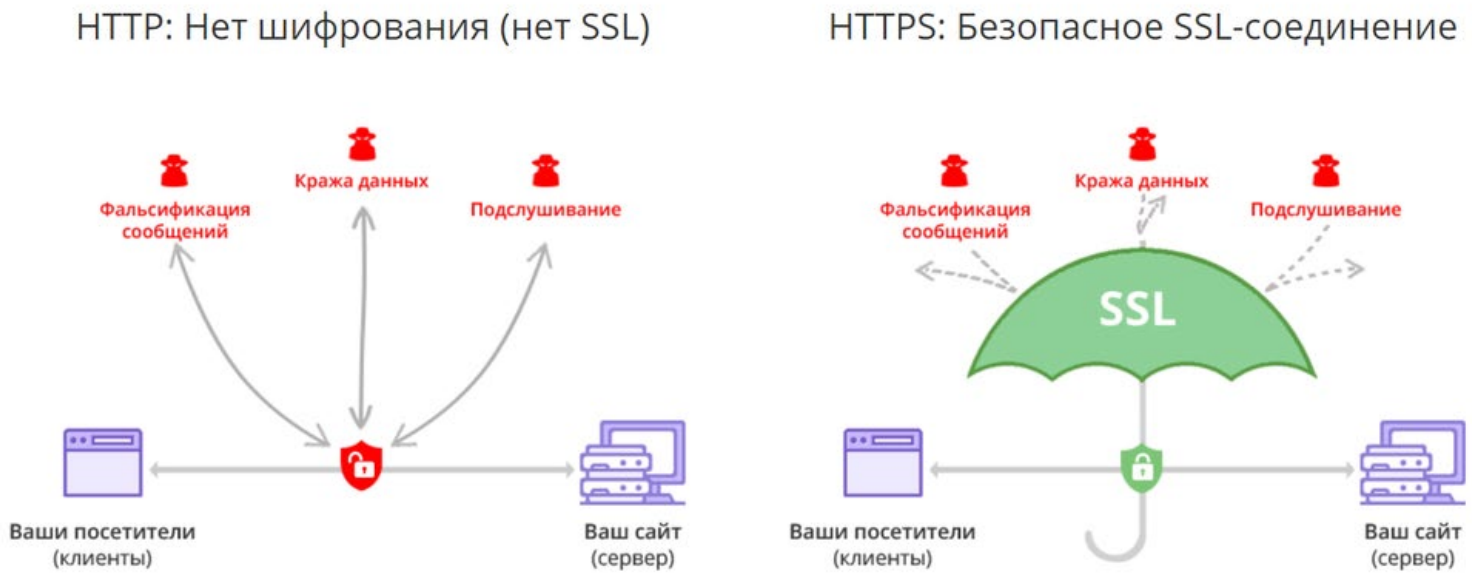
КРИПТОПРО

Веб-доступ к сайтам (WEB TLS)

VPN – доступ к произвольным ресурсам (Point-to-Site)

VPN – доступ между площадками (Site-to-Site)

Защищенные и незащищенные соединения



- HTTP – протокол **незащищенного** обмена данными между пользователем и сайтом
- HTTPS – расширение протокола HTTP, обеспечивающее **защиту** обмена данными
- TLS – протокол, реализующий защиту в HTTPS-соединении с помощью **сертификатов**

Два равноправных пути развития TLS в России

SSL/TLS с RSA

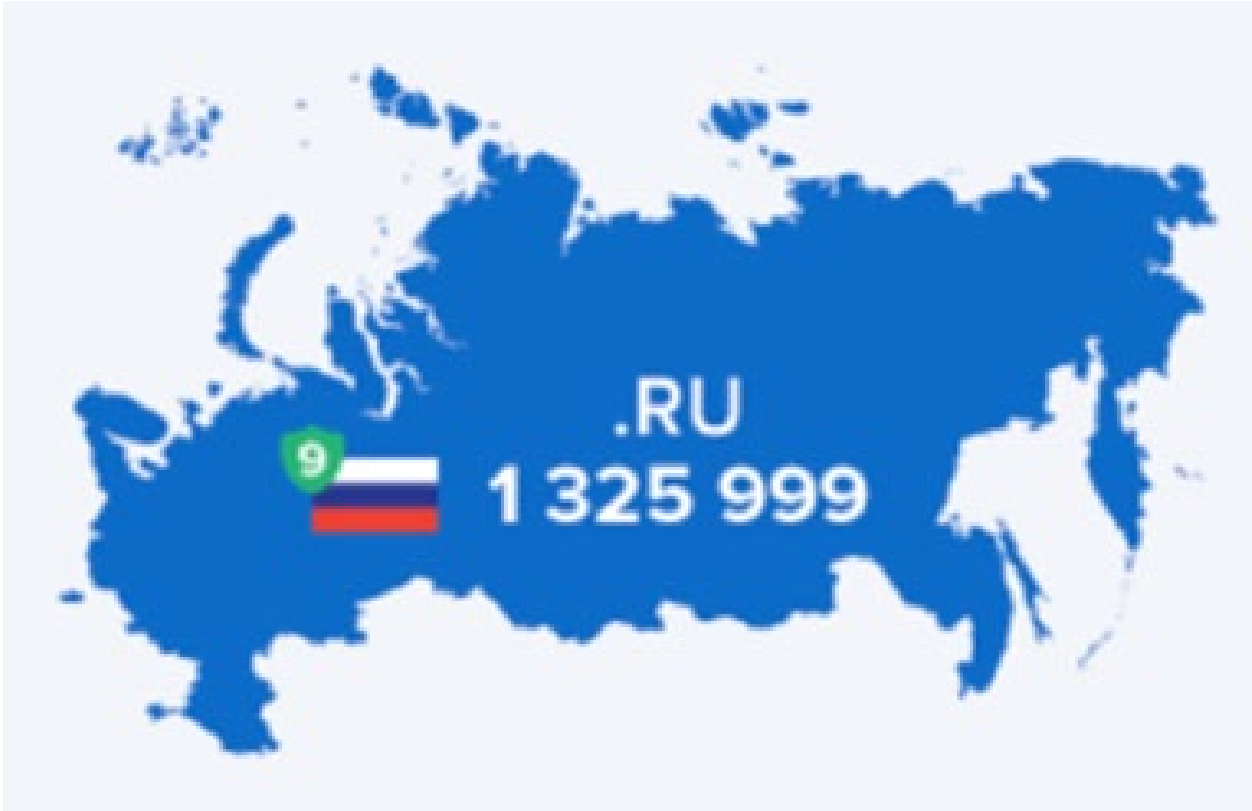
- RFC
- Поддержка со стороны браузеров
- Удостоверяющие центры
- Серверные решения (шлюзы)

TLS с ГОСТ

- RFC
- Поддержка со стороны браузеров
- Удостоверяющие центры
- Серверные решения (шлюзы)

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:

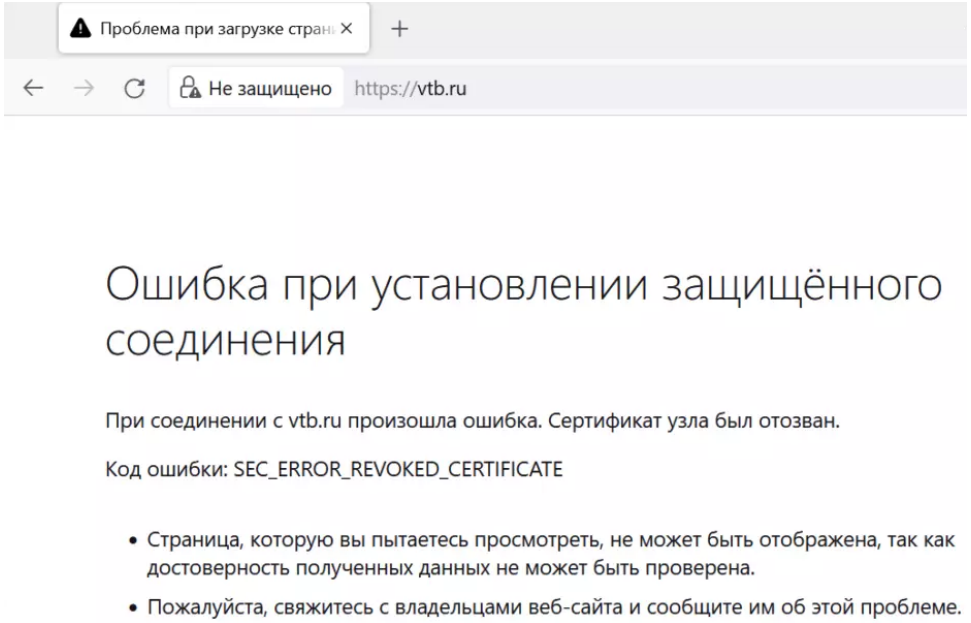
- Отзыв действующего сертификата
- Утрата доверия к корневому сертификату

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



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

Коммерческие зарубежные УЦ:

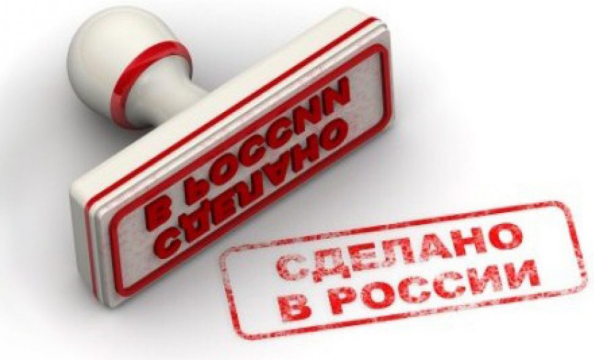
- Бельгия: https://www.globalsign.com
- Турция: https://e-tugra.com.tr/ssl-sertifikasi
- Италия: https://www.actalis.com/it/home.aspx
- Китай: https://www.cfca.com.cn/20150810/100002755.html

Некоммерческие зарубежные УЦ:

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

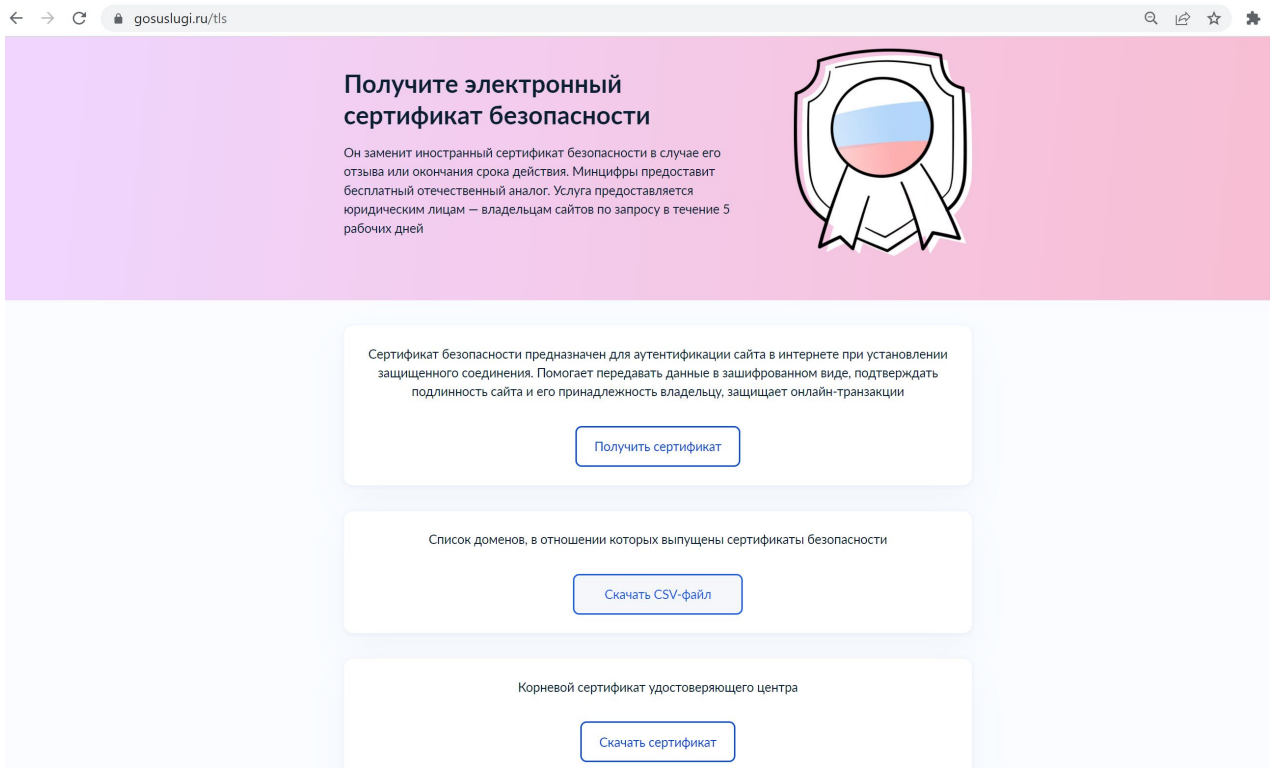
Законодательное обеспечение ГОСТ TLS

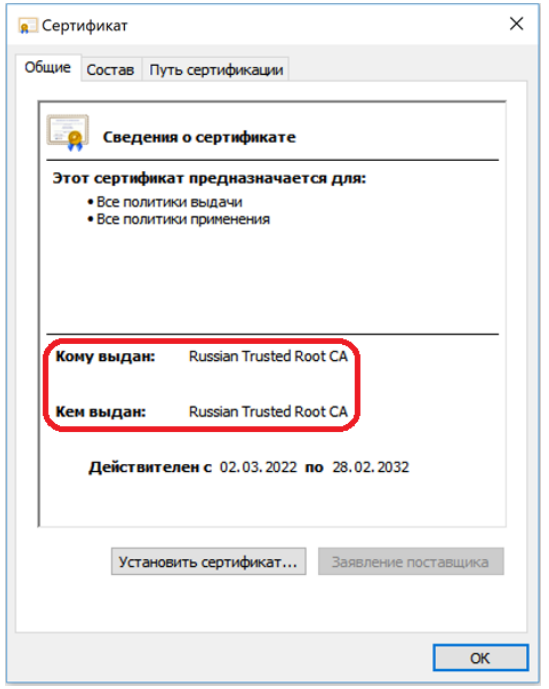
- **2016.** Поручение Президента (Пр-1380) про переход ОГВ на российскую криптографию
- **2017.** Программа «Цифровая экономика РФ»
- **2018.** Дорожные карты по переходу на ГОСТ в Рунете
- **2020.** Пилотный проект по использованию российских алгоритмов и шифрсредств в ГИС
- **2022.** Ожидается принятие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

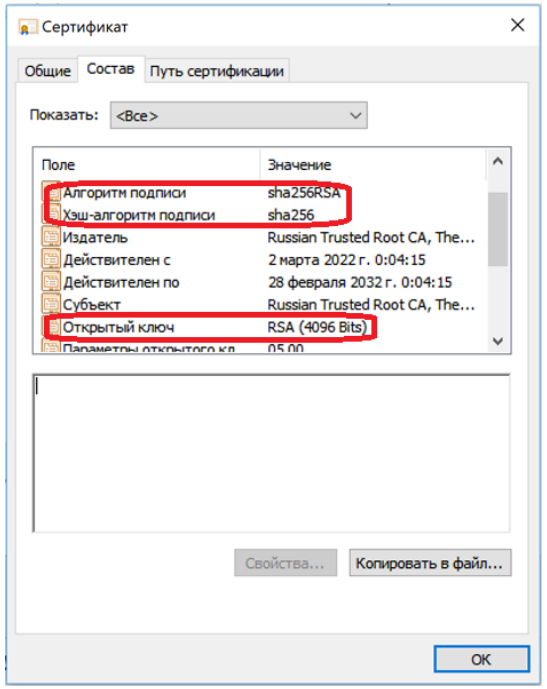


Стандартный вариант – TLS-сертификат (RSA) от НУЦа

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 корневым 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 ошибка и браузер не даст посетить сайт

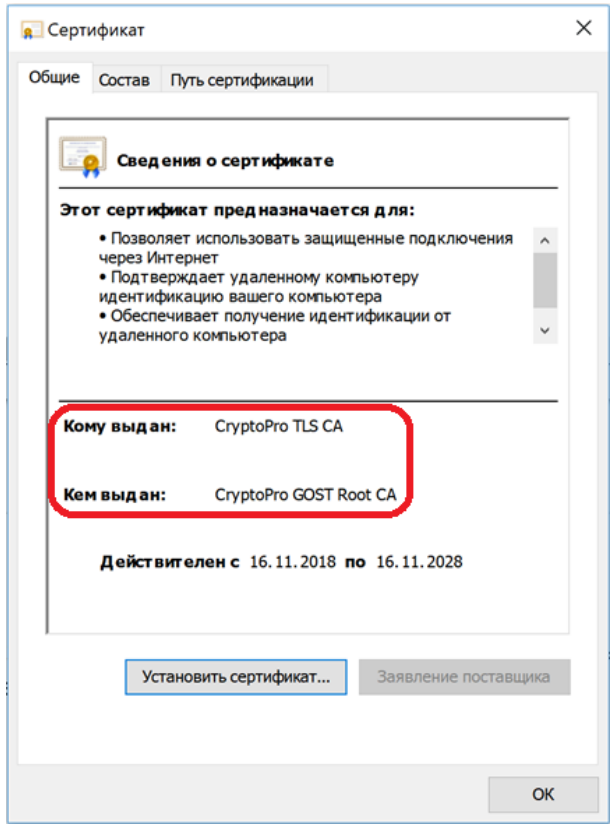
Доверие к корневым сертификатам в КриптоПро CSP

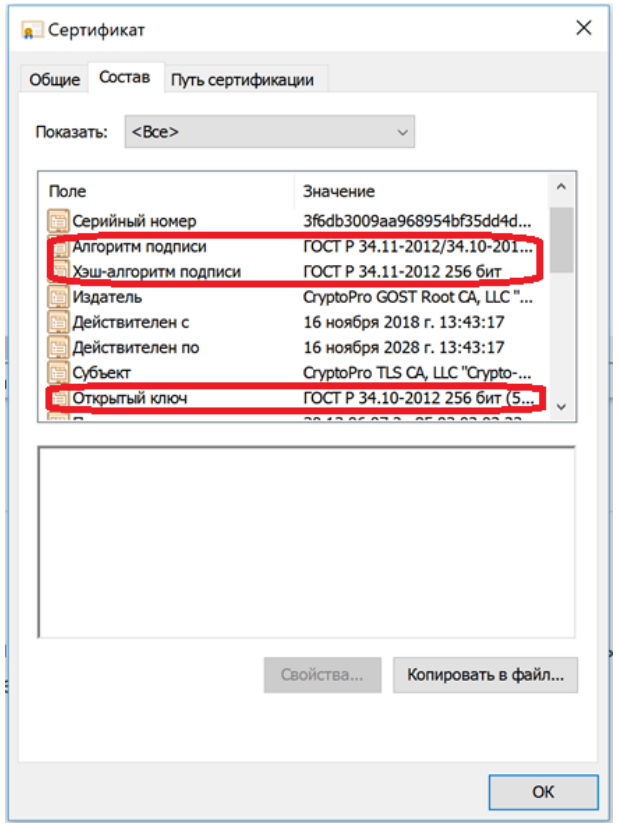
В актуальной версии КриптоПро CSP 5.0 R3 обеспечена поддержка корневых сертификатов:

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

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

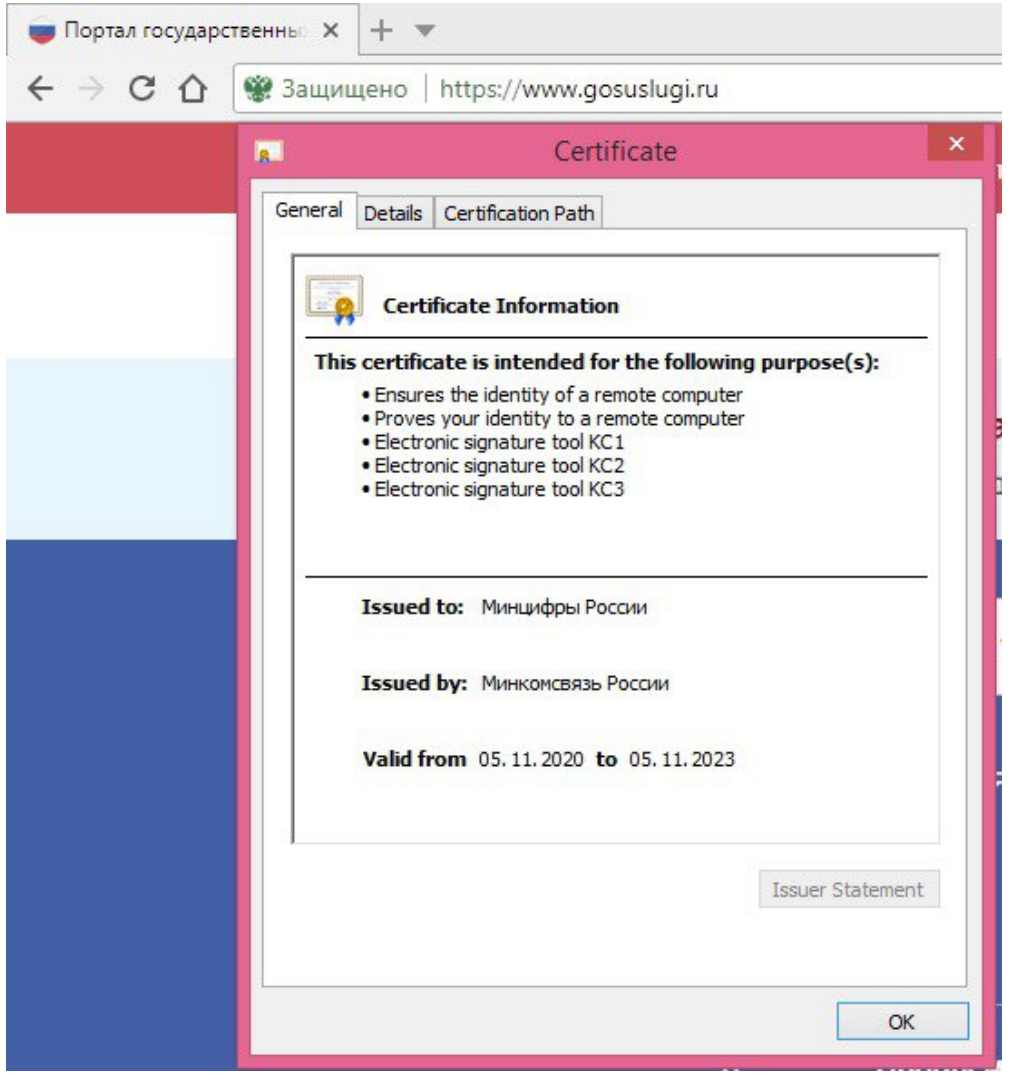




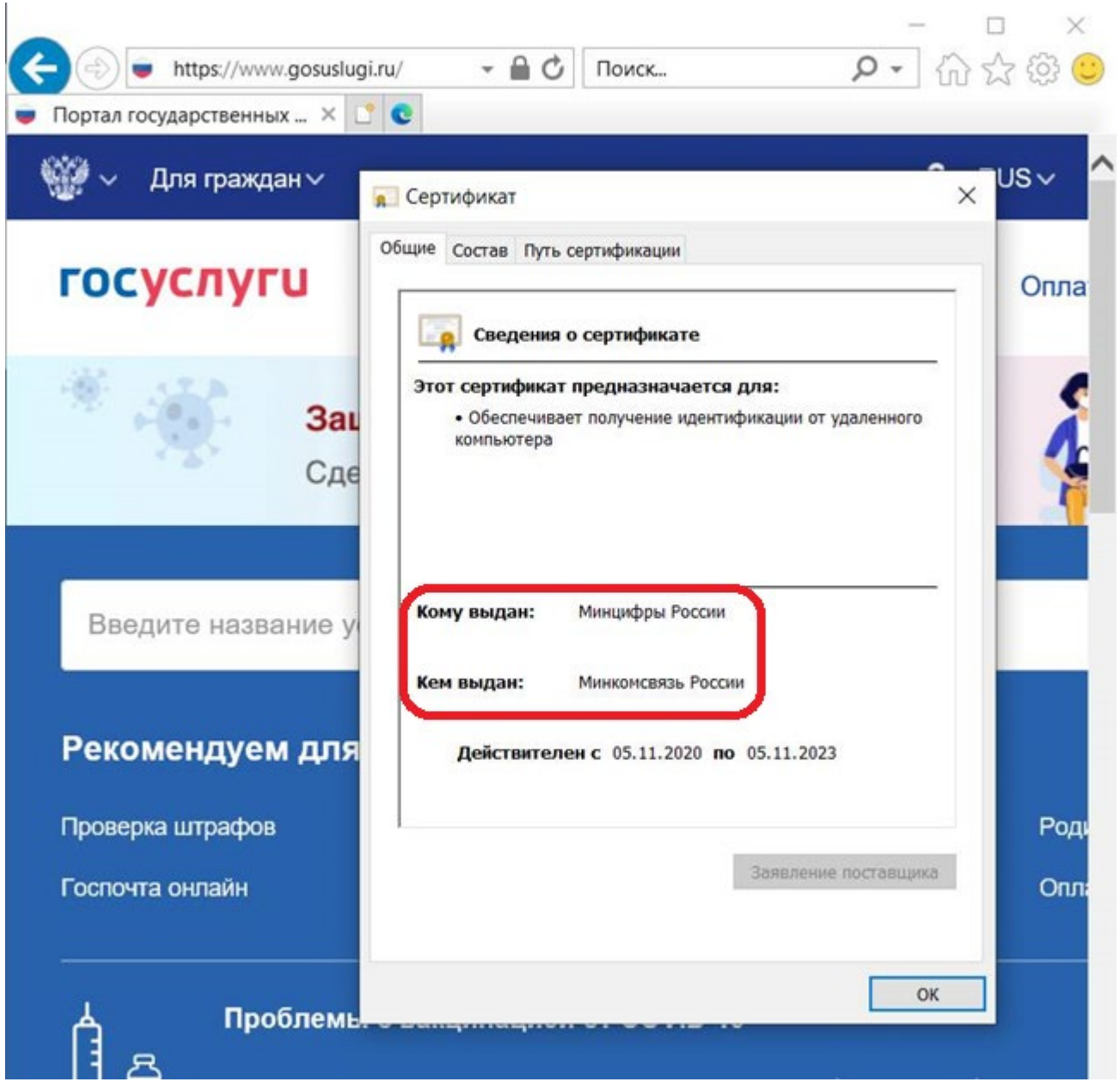
Поддержка ГОСТ TLS на веб-сайтах (примеры)

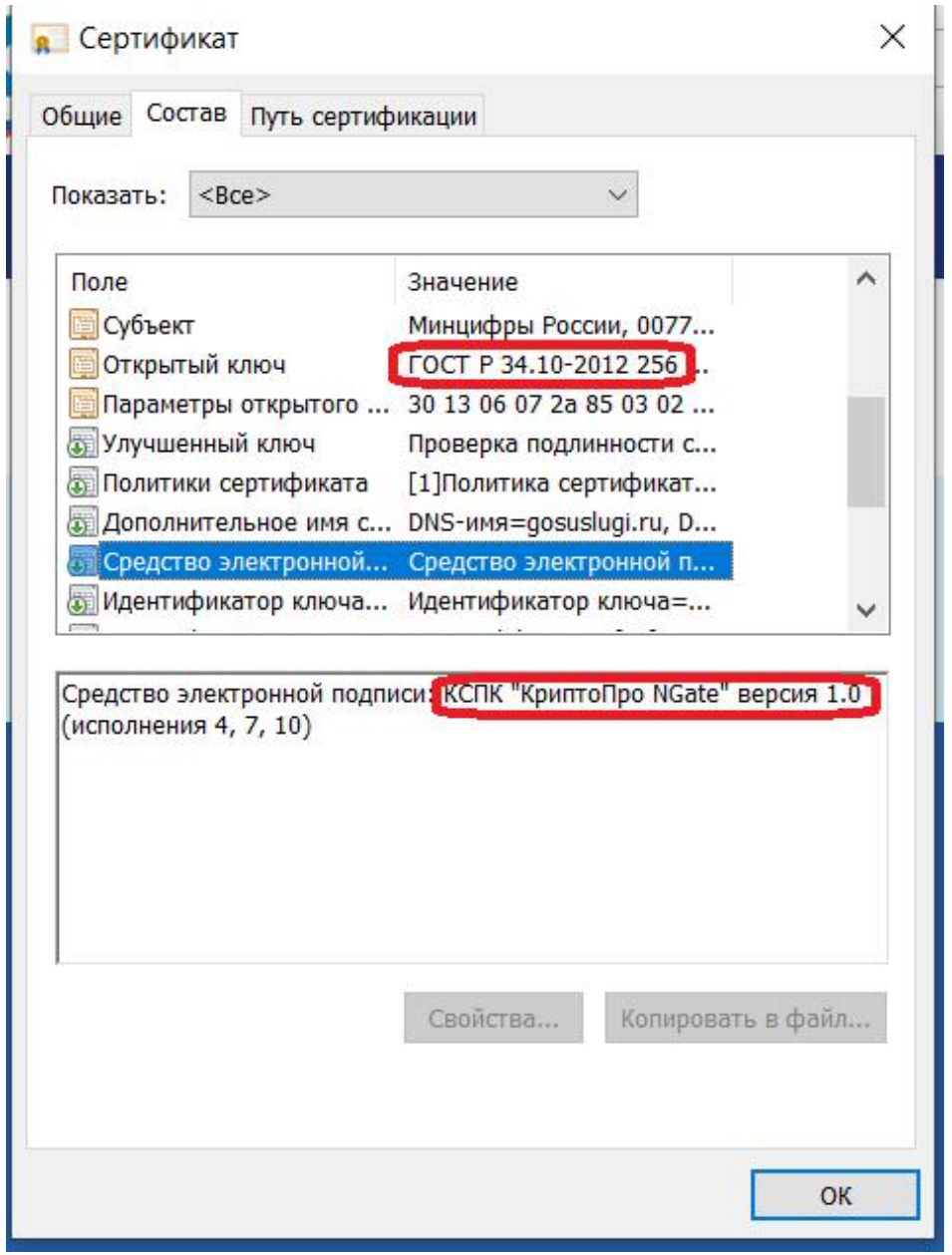
Защищено

- 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

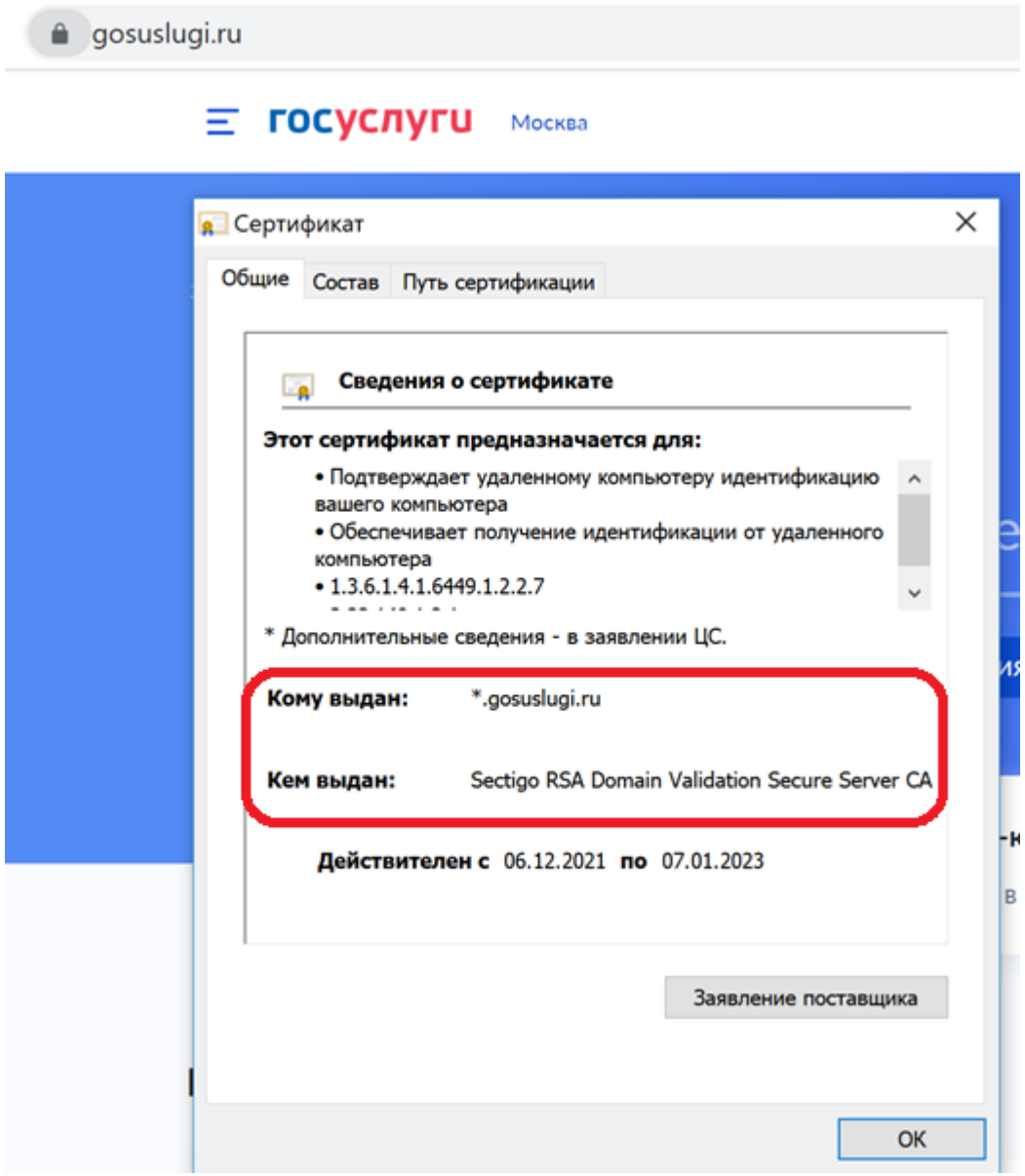


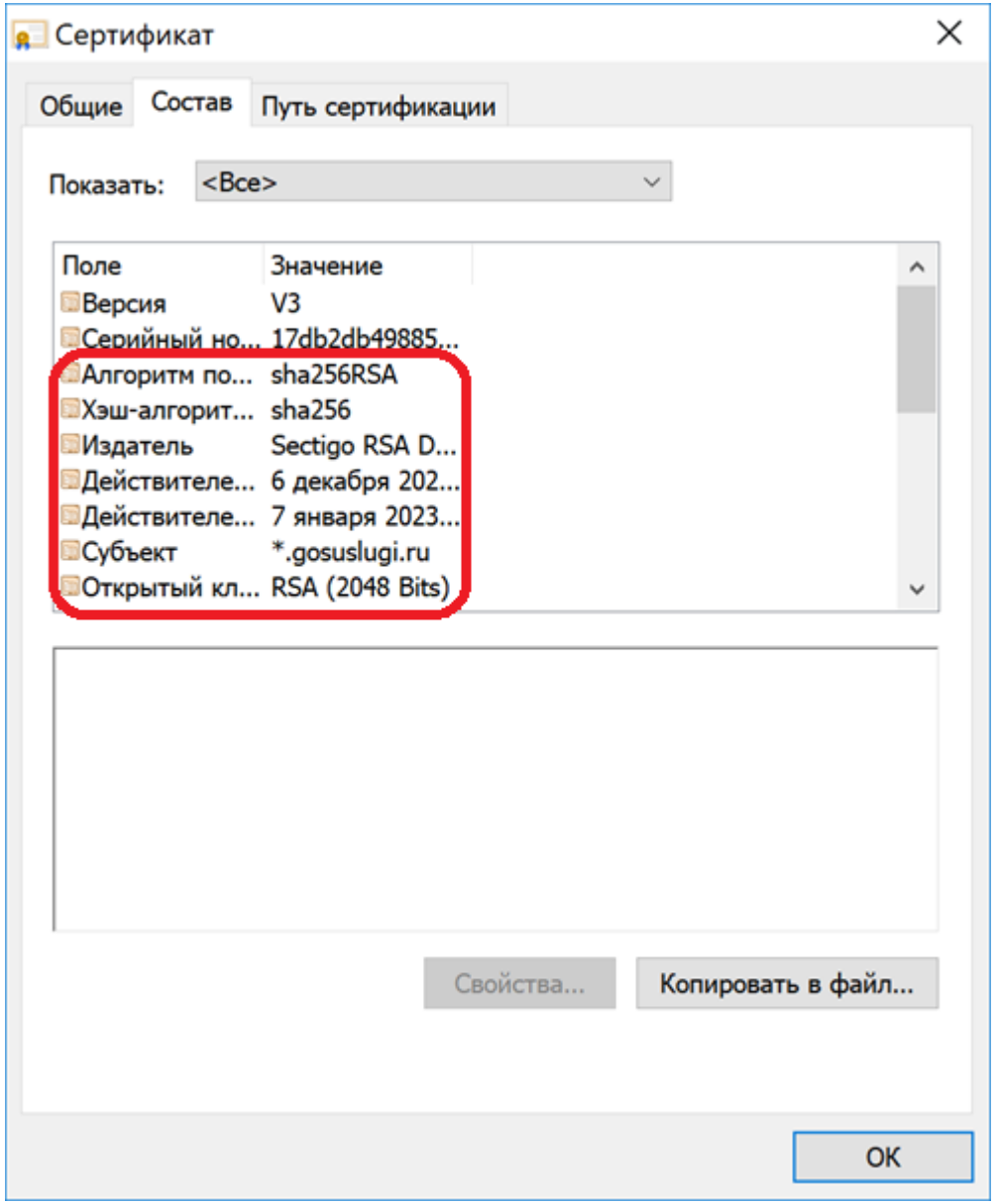
Пример - доступ к ПГУ с браузеров, поддерживающих ГОСТ





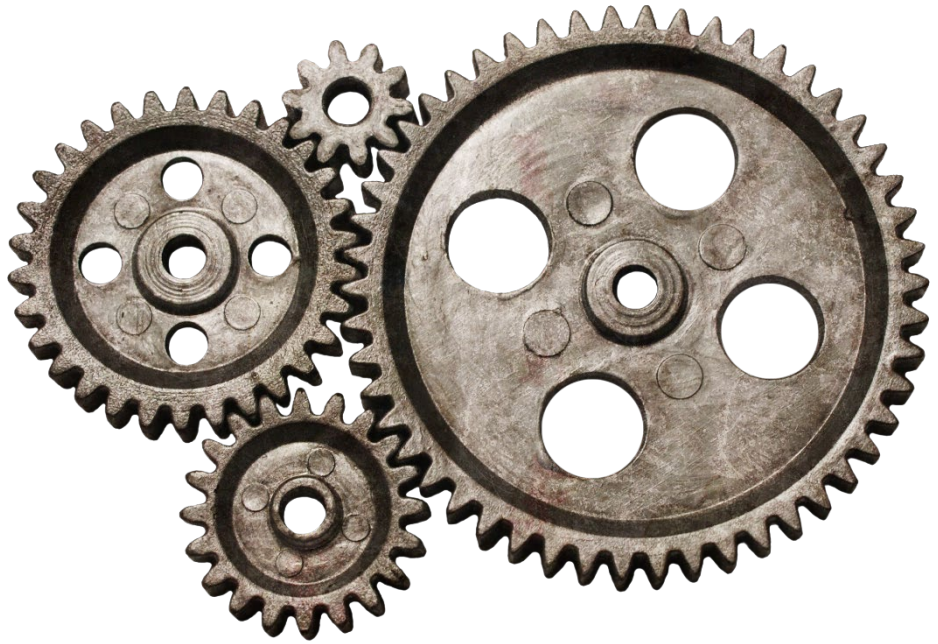
Пример - доступ к ПГУ с браузеров, не поддерживающих ГОСТ



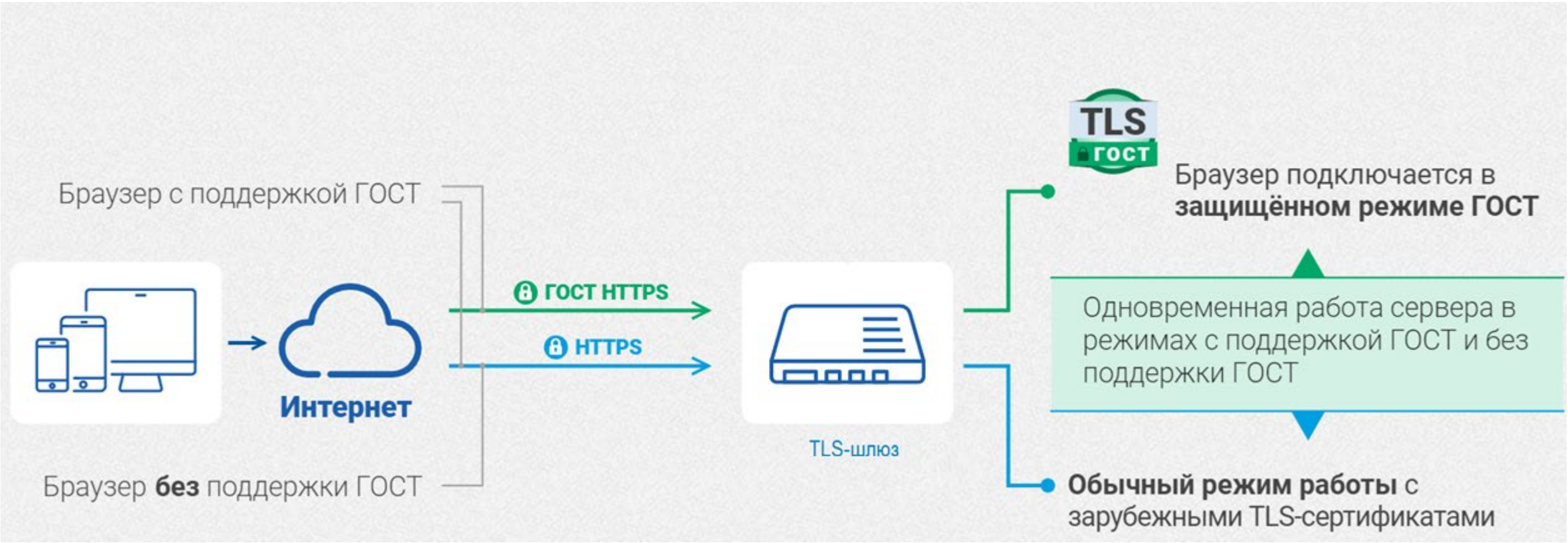


Требуемые компоненты для работы ГОСТ TLS

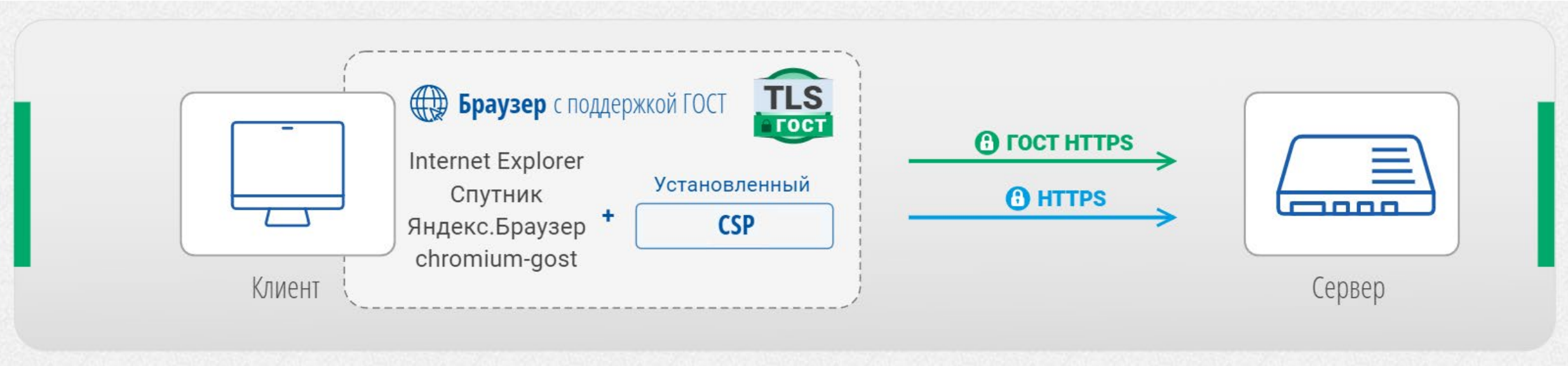
- TLS-сервера с одновременной поддержкой ГОСТ и не ГОСТ
- Браузеры с поддержкой ГОСТ TLS
- Мобильные приложения с поддержкой ГОСТ TLS



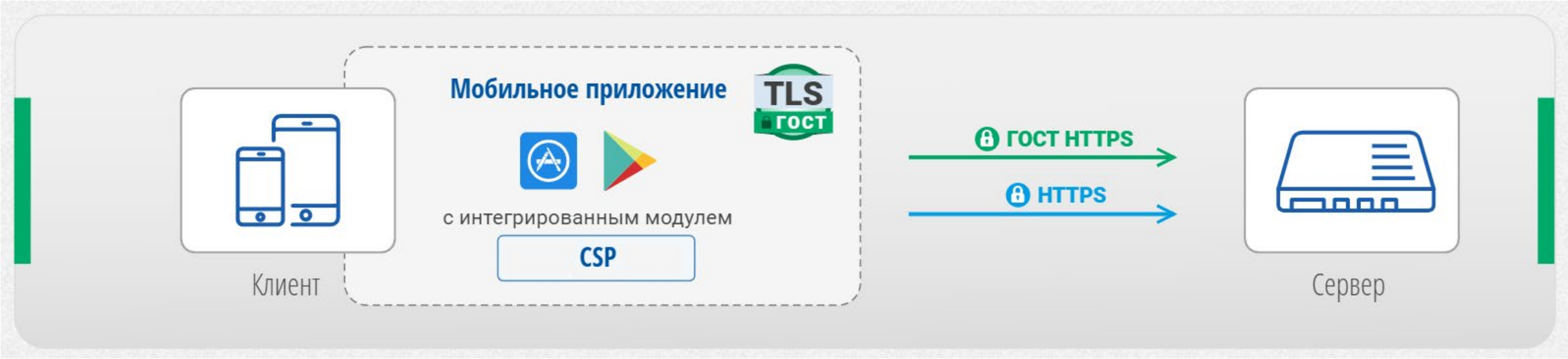
Постепенный переход на ГОСТ TLS



Клиентские решения для стационарных устройств



Клиентские решения для мобильных устройств



Веб-доступ к сайтам (WEB TLS)

VPN – доступ к произвольным ресурсам (Point-to-Site)

VPN – доступ между площадками (Site-to-Site)

VPN-доступ


VPN-туннель
Интернет
NG
КриптоПро NGate
Произвольный
IP-трафик
Внутренние
корпоративные
сервисы

Замена зарубежных решений

№	Функция (характеристика)	КриптоПро NGATE
1	SSL VPN (TLS)	**Да**
3	IPSEC VPN	**Да**
4	Поддержка не менее 20 000 одновременных сессий (на одном шлюзе)	**Да**
5	Пропускная способность одного VPN-шлюза не менее 10 Гбит/с	**Да**
7	Возможность масштабирования решения	**Да**
8	Auto-reconnect VPN, без необходимости ввода учетных данных	**Да**
9	Запрет взаимодействия между пользователями, подключенными к VPN	**Да**
11	"Always-On" (предоставляет возможность предотвратить прямой доступа в Интернет, если устройство не подключено к корпоративной сети)	**Да**
12	Split-tunneling: возможность отправлять в туннель только трафик до определенных сетей, весь остальной трафик исключить	**Да**
13	Split-tunneling: возможность отправлять в туннель весь трафик, за исключением определенных сервисов (исключение на основе IP-адресов)	**Да**
15	Возможность формирования различных профилей подключений с предустановленными настройками для VPN-клиентов	**Да**
16	Возможность выбора определённого профиля при подключении к VPN	**Да**
17	Ограничение количества разрешенных одновременных сессий для одной учетной записи, в рамках одного профиля VPN (в рамках одного шлюза)	**Да**
18	Возможность аутентификации с использованием цифровых сертификатов	**Да**
19	Возможность интеграция с Microsoft AD, LDAP	**Да**
20	Возможность ограничени доступа к ресурсам сети на основе ролевой модели	**Да**
21	Возможность смены пароля доменной учетной запсиси при подключении к VPN, в случае истечения срока действия пароля учетной записи	**Да**
22	Возможность интеграции со средствами 2ФА (через Radius)	**Да**
24	Поддержка работы VPN-клиента в ОС Windows	**Да**
25	Поддержка работы VPN-клиента в ОС Linux	**Да**
26	Поддержка работы VPN-клиента в ОС macOS	**Да**
27	Поддержка функционала оценки состояния устройства пользователя	**Да** (Сакура/SafeMobile)
28	Ограничение доступа к сети при несоответствии требованиями политики ИБ	**Да** (Сакура/SafeMobile)
29	Перечень возможных проверок в рамках процедуры оценки состояния	**Да** (Сакура/SafeMobile)
30	Осуществляет ли вендор поддержку в РФ	**Да**

NGate + Сакура (ПК) и NGate + SafePnone (моб)

Веб-доступ к сайтам (WEB TLS)

VPN – доступ к произвольным ресурсам (Point-to-Site)

VPN – доступ между площадками (Site-to-Site)

VPN-доступ к произвольным ресурсам (Site-to-Site)

Основные преимущества NGate

- Единое устройство для всех видов доступа
- Point-to-site доступ по протоколу TLS
- Site-to-site доступ по стандартному протоколу IPSec
- Наличие сертификатов ФСБ по классам КС1, КС2, КС3
- Одновременная поддержка ГОСТ и не ГОСТ подключений
- Поддержка всех современных ОС, в т.ч. мобильных
- Многофакторная аутентификация (AD, LDAP, RADIUS, сертификаты)
- Высокая производительность (до 45000 одновременных подключений)

КРИПТОПРО

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**