

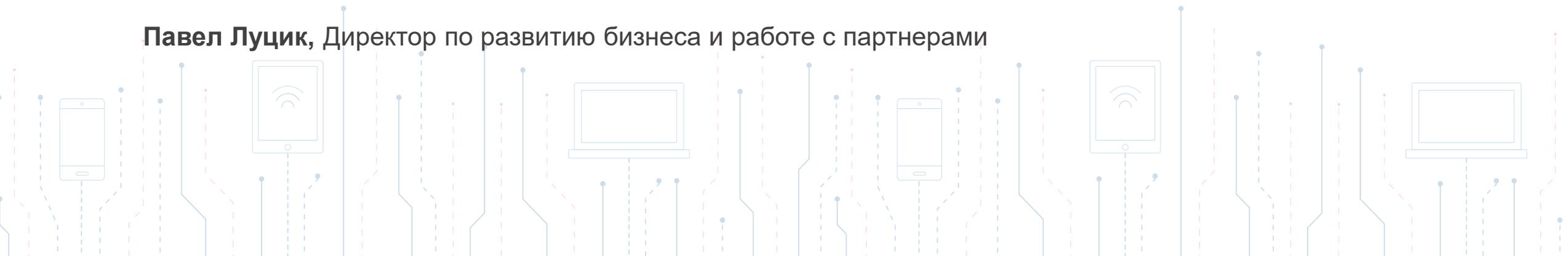


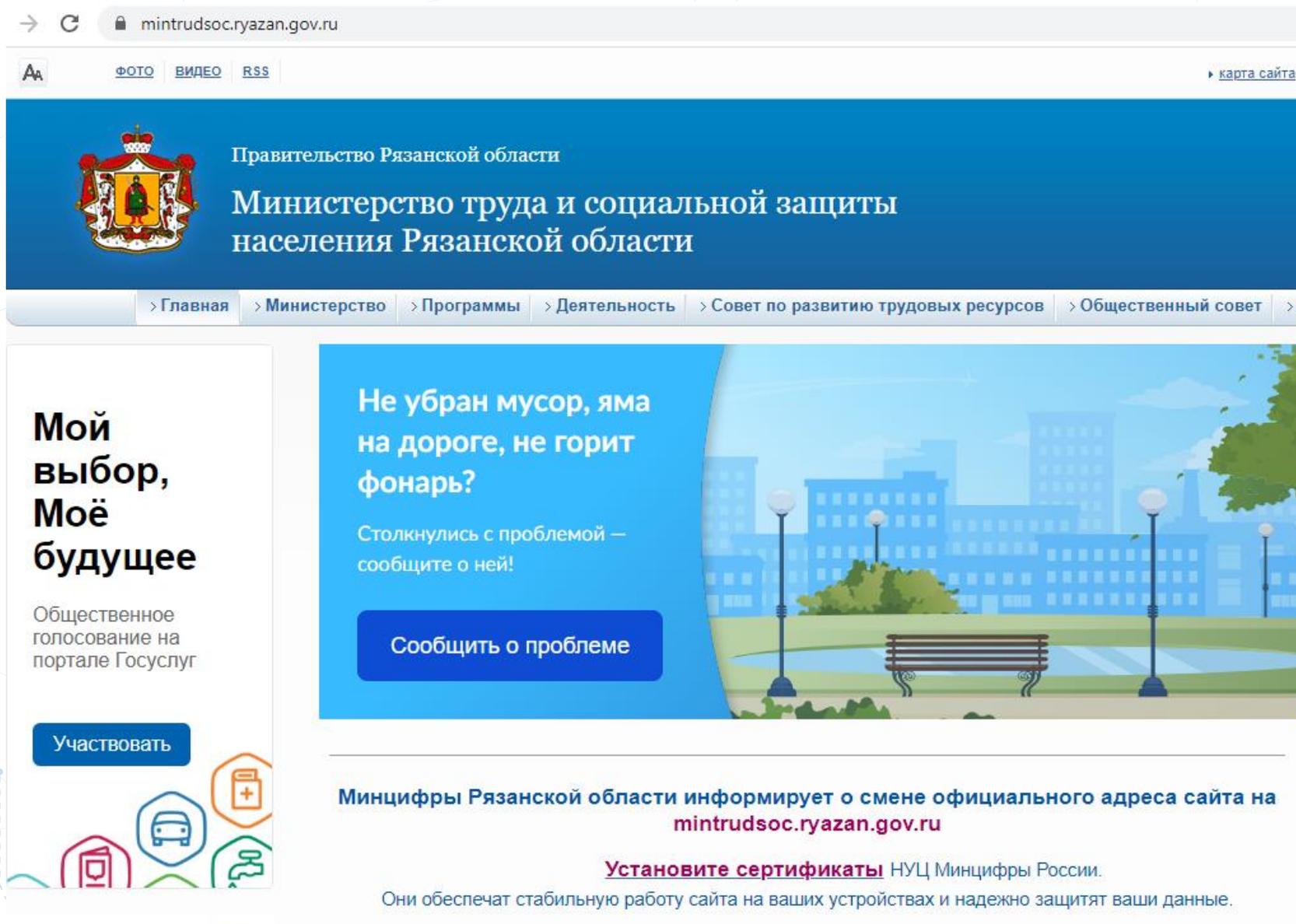
Ключевое слово
в защите информации



Комплексное импортозамещение средств защищенного удаленного доступа

Павел Луцик, Директор по развитию бизнеса и работе с партнерами





→ ↻ mintrudsoc.ryazan.gov.ru

Аа ФОТО ВИДЕО RSS [карта сайта](#)

 Правительство Рязанской области
Министерство труда и социальной защиты населения Рязанской области

[Главная](#) [Министерство](#) [Программы](#) [Деятельность](#) [Совет по развитию трудовых ресурсов](#) [Общественный совет](#)

Мой выбор, Моё будущее
Общественное голосование на портале Госуслуг
[Участвовать](#)

Не убран мусор, яма на дороге, не горит фонарь?
Столкнулись с проблемой — сообщите о ней!
[Сообщить о проблеме](#)

Минцифры Рязанской области информирует о смене официального адреса сайта на mintrudsoc.ryazan.gov.ru
Установите сертификаты НУЦ Минцифры России.
Они обеспечат стабильную работу сайта на ваших устройствах и надежно защитят ваши данные.

<https://mintrudsoc.ryazan.gov.ru>



▶ Тренды

CSP

UPM-сервер

HSM

СКЭМ

Электронная
подпись

- Импортозамещение
- Переходу на TLS с ГОСТ
- Пандемия, переход на «удаленку»



- Пр-1380 от 16.07.2016 (О переводе госорганов на отечественную криптографию)
- Нацпроект от 01.10.2018 (Цифровая экономика)
- 1236-ПП от 16.11.2015 (Об установлении запрета на допуск иностранного ПО)
- 166-УП от 30.03.2022 (О мерах по обеспечению технологической независимости и безопасности КИИ РФ)
- 250-УП от 01.05.2022 (О дополнительных мерах по обеспечению ИБ РФ)

С 31.03.2022 запрещено закупать иностранное ПО

С 01.01.2025 запрещено использовать иностранное ПО

▶ Доступ к веб-сайтам

Электронная
подпись

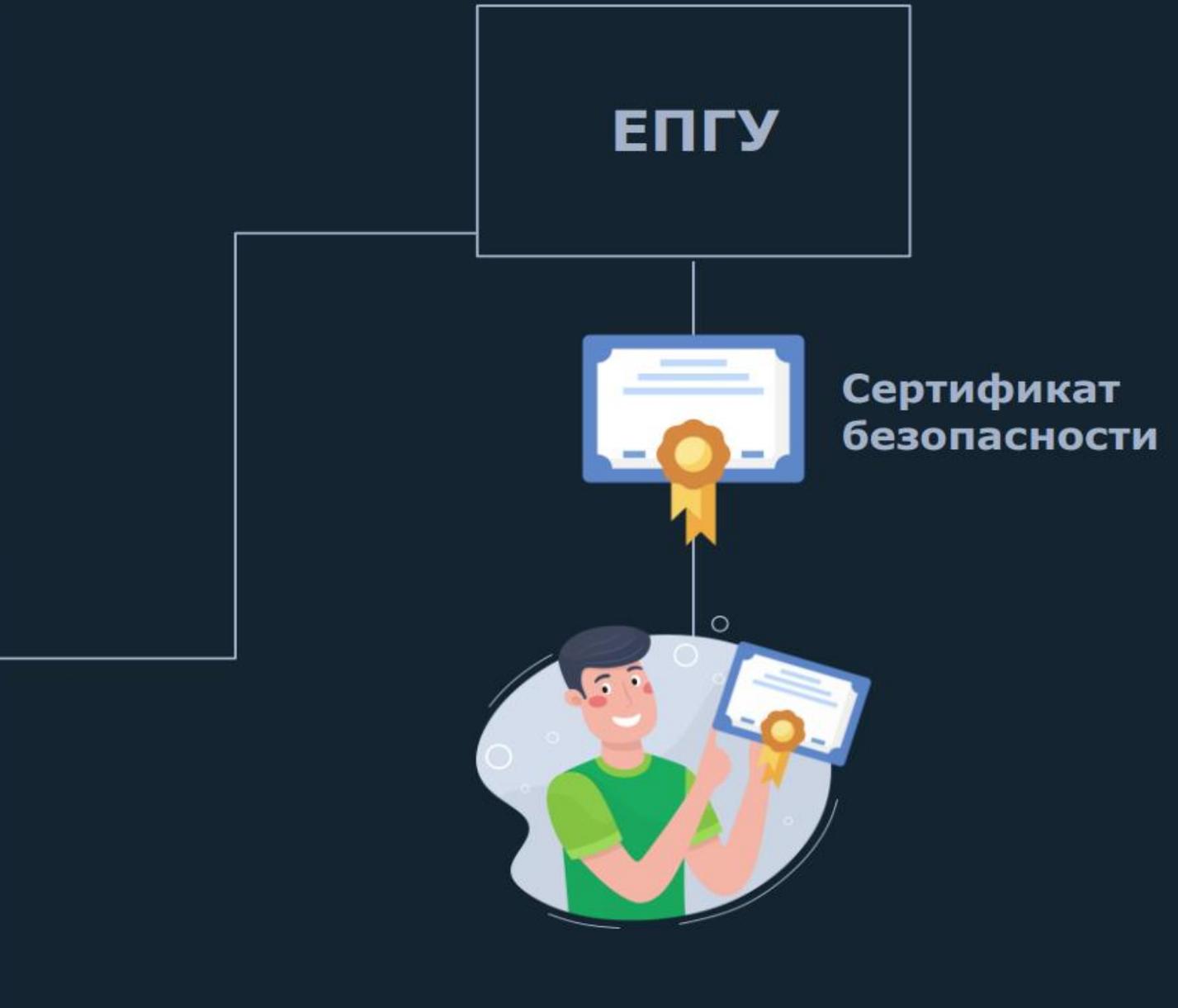
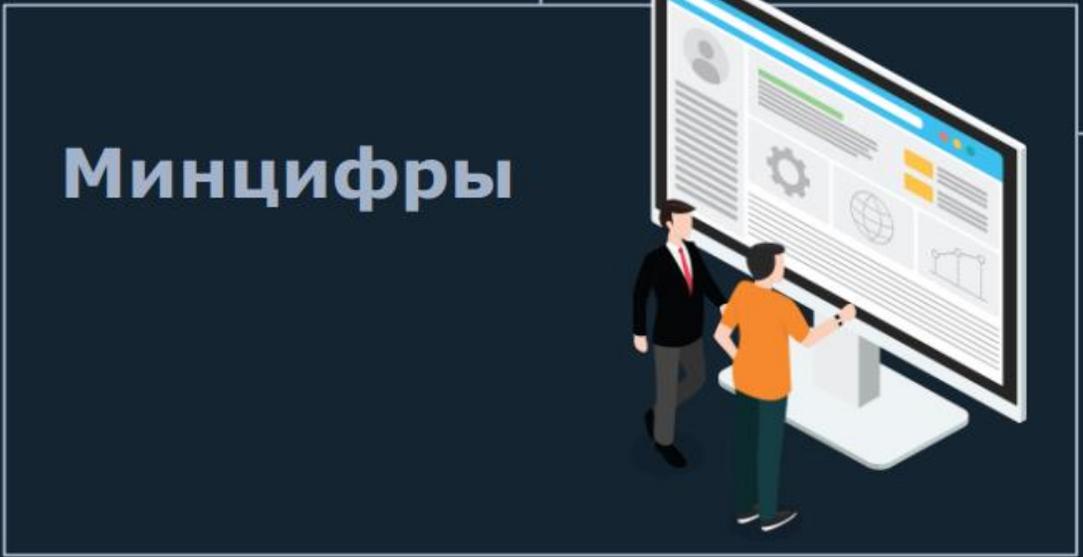
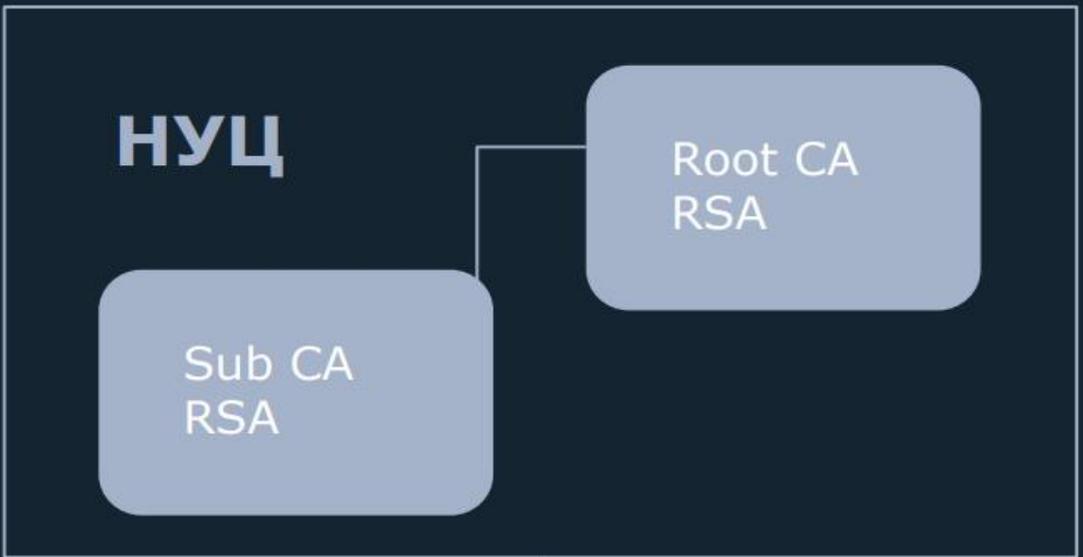
HSM

CSP

UPM-
сервер

СКЭМ

- 2017 – Утрата доверия Google к сертификатам от Symantec
- 2018 – Отозван сертификат Общественной палаты РФ
- 2022 – Отозваны сертификаты у ВТБ, ЦБ, ПСБ, Сбербанк, МО
- 2022 – Прекращена выдача сертификатов для Рунета со стороны УЦ Sectigo (бывш. Comodo), DigiCert, Thawte, Rapid, GeoTrust
- 2022 – введен в действие НУЦ для выдачи RSA-сертификатов



gosuslugi.ru/tls

госуслуги Москва

Получите электронный сертификат безопасности

Он заменит иностранный сертификат безопасности в случае его отзыва или окончания срока действия. Минцифры предоставит бесплатный отечественный аналог. Услуга предоставляется юридическим лицам — владельцам сайтов по запросу в течение 5 рабочих дней

Сертификат безопасности предназначен для аутентификации сайта в интернете при защищенного соединения. Помогает передавать данные в зашифрованном виде, подтверждает подлинность сайта и его принадлежность владельцу, защищает онлайн-тран

доменов, в отношении которых выпущены сертификаты безопасн

Корневой сертификат удостоверяющего центра

Получить сертификат

Скачать CSV-файл

Скачать сертификат

<https://www.gosuslugi.ru/tls>

Сертификат

Общие Состав Путь сертификации

Сведения о сертификате

Этот сертификат предназначен для:

- Все политики выдачи
- Все политики применения

Кому выдан: Russian Trusted Root CA

Кем выдан: Russian Trusted Root CA

Действителен с 02.03.2022 по 28.02.2032

Установить сертификат... Заявление поставщика

OK

	A
3607	aztlan.banksoyuz.ru
3608	*.intercompglobal.com
3609	*.bss.2gis.com
3610	*.cryptocom.ru
3611	mab.banksoyuz.ru
3612	sppltd.ru
3613	ffin.ru
3614	demo.faktura.ru
3615	*.obdt.intercomp.ru
3616	mail.roscartography.ru
3617	*.egais.plus
3618	fin.roscartography.ru
3619	mx1.rt-solar.ru
3620	ftp.roscartography.ru
3621	v.ms-box.ru
3622	*.intercomp.kz
3623	*.sberavtopark.ru
3624	www.asmud.banksoyuz.ru
3625	*.uslugi.gov39.ru
3626	*gov39.ru
3627	gov39.ru
3628	*.flamp.ru
3629	www.bonus.banksoyuz.ru
3630	*.api.2gis.com
3631	mv-exway-e.banksoyuz.ru
3632	maps.2gis.com
3633	www.amelia-st.ru
3634	soglasie.ru
3635	*.2gis.one
3636	inti.banksoyuz.ru
3637	photo.2gis.com
3638	*.sber-solutions.group
3639	api.2gis.com
3640	2gis.by
3641	flamp.ru
3642	grandsmeta.store

Поддержка работы сайтов с российскими сертификатами

Для получения защищённого доступа ко всем сайтам и онлайн-сервисам используйте браузеры с поддержкой российских сертификатов: Яндекс Браузер или Атом

Скачать Яндекс Браузер

Скачать Атом

Альтернативный способ — установка корневого сертификата

Если вы привыкли работать в других браузерах или возникли проблемы с работой сторонних программ, вы можете установить корневой сертификат в операционную систему

Сертификаты для Android

Сертификаты для iOS

Сертификаты для Windows

Сертификаты для MacOS

Сертификаты для Linux

<https://www.gosuslugi.ru/crt>



SBER PRESS

Москва

Войти



Сбер начал перевод своих сайтов на российские сертификаты удостоверяющих центров

Поделиться    

#Технологии #Официальное

Сбер первым в стране начал установку сертификатов, выпущенных Удостоверяющим центром Минцифры на все свои сайты, а также рабочие ресурсы и системы.

Данное решение обеспечит независимость банка от зарубежных удостоверяющих центров и гарантирует пользователям безопасный доступ к ресурсам Сбера.

Сбер постоянно ведёт работу по замещению зарубежных вендоров и сервисов на отечественные разработки. В рамках этой программы мы первыми в стране начали заменять зарубежные сертификаты на отечественные. В ближайшее время на них будет переведён наш главный сайт sberbank.ru. Также на российские сертификаты перейдут и остальные сайты, ресурсы и системы Сбера. Это гарантирует бесперебойный и безопасный доступ наших клиентов к сервисам банка, обеспечивая их независимость от иностранных решений

Герман Греф
Президент, Председатель Правления Сбербанка

sberbank.ru/person

СБЕР БАНК Частным клиентам Самозанятым Малому бизнесу и ИП Ещё

Курсы валют Офисы Банкоматы Москва ENG СБЕР

SberPay > новое СберПрайм+ > Кредиты Ипотека Карты Вклады Премиум > Инвестиции Платежи Переводы Страхование

Детская СберКарта

Успейте оформить карту с Чебурашкой!

[Подробнее](#)

Вам может понравиться

Вклады

СберВклад

[Открыть вклад >](#)

Вклады

Вклад «Лучший %»

[Оформить онлайн >](#)

Дебетовые карты

СберКарта

[Оформить онлайн >](#)

Сертификат

Общие Состав Путь сертификации

Сведения о сертификате

Этот сертификат предназначен для:

- Обеспечивает получение идентификации от удаленного компьютера

Кому выдан: sberbank.ru

Кем выдан: Russian Trusted Sub CA

Действителен с 26.09.2022 по 26.09.2023

[Установить сертификат...](#) [Заявление поставщика](#)

[OK](#)

→ ↻ mintrudsoc.ryazan.gov.ru

Аа ФОТО ВИДЕО RSS



Правительство Рязанской области
Министерство труда и социальной защиты населения Рязанской области

> Главная > Министерство > Программы > Деятельность > Совет по развитию трудовых рес

Мой выбор, Моё будущее

Общественное голосование на портале Госуслуг

Участвовать

Не убран мусор, яма на дороге, не горит фонарь?

Столкнулись с проблемой — сообщите о ней!

Сообщить о проблеме

Минцифры Рязанской области информирует о смене официальной почты: mintrudsoc.ryazan.gov.ru

Установите сертификаты НУЦ Минцифры Рязанской области. Они обеспечат стабильную работу сайта на ваших устройствах и надежную защиту ваших данных.

Сертификат

Общие Состав Путь сертификации

Сведения о сертификате

Этот сертификат предназначен для:

- Обеспечивает получение идентификации от удаленного компьютера

Кому выдан: *.ryazan.gov.ru

Кем выдан: Russian Trusted Sub CA

Действителен с 28.12.2022 по 28.12.2023

Установить сертификат... Заявление поставщика

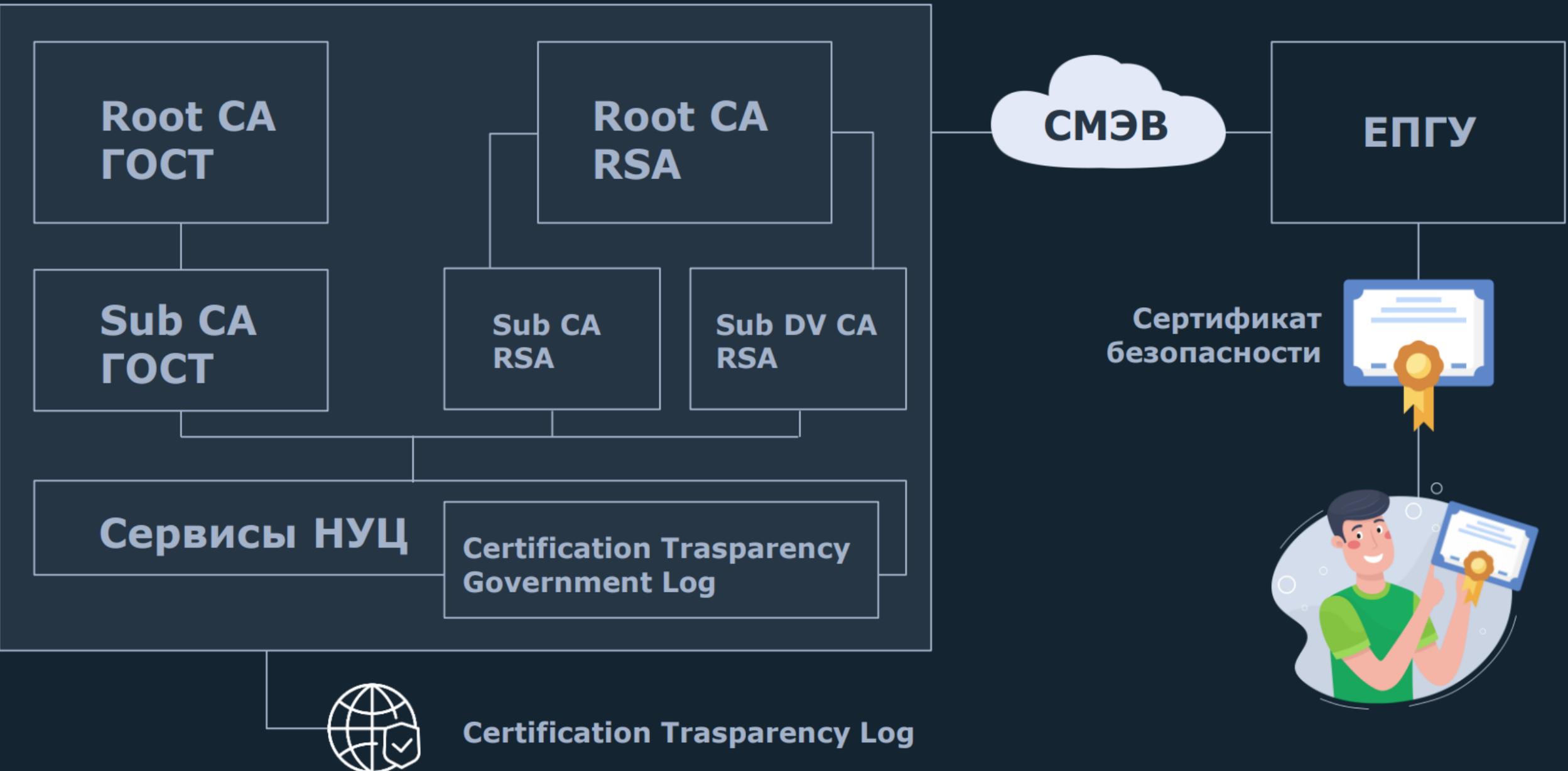
OK

SSL/TLS с RSA

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

TLS с ГОСТ

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



Получение сертификата ГОСТ TLS

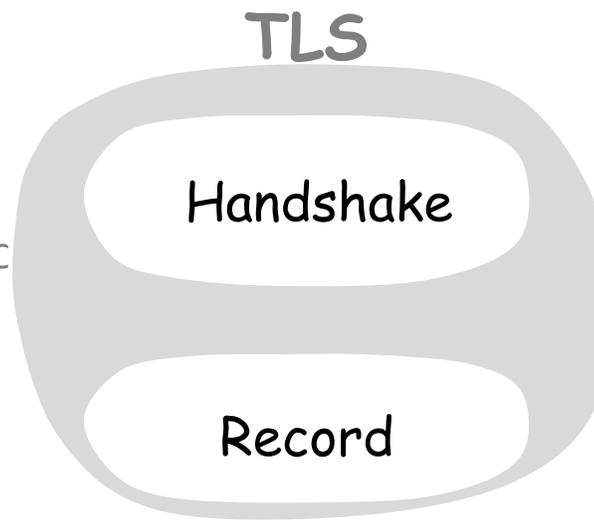
Удостоверяющего центра CryptoPro TLS CA



Удостоверяющий центр
CryptoPro TLS CA



TLS_GOSTR341112_256_WITH_28147_CNT_IMIT
 TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC
 TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC



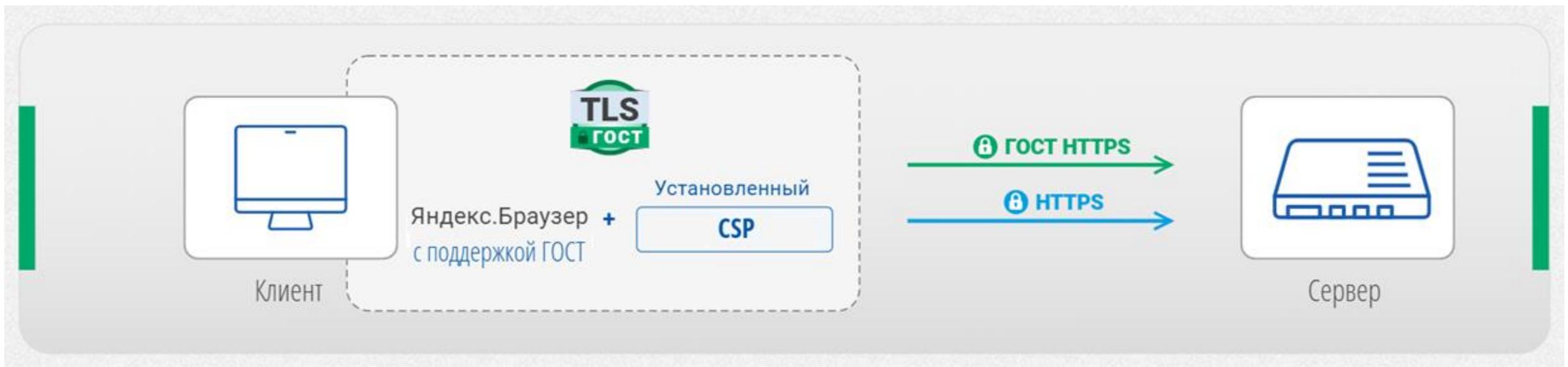
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
 TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
 TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
 TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

TLS 1.2 с ГОСТ

- ✓ P 1323565.1.020-2020
- ✓ RFC 9189
- ✓ Идентификаторы в реестре IANA

TLS 1.3 с ГОСТ

- ✓ P 1323565.1.030-2020
- ✓ RFC 9367
- ✓ Идентификаторы в реестре IANA



gosuslugi.ru/browser

госуслуги Москва

Помощь Войти Регистрация

Пакет программ для безопасного голосования

Скачайте браузер с шифрованием данных по ГОСТ TLS.
 Для Windows уже включён КриптоПро CSP.
 Для Linux КриптоПро нужно [скачать отдельно](#)

 Windows	 Linux deb	 Linux rpm
Уже включён КриптоПро CSP	Astra Linux, Debian, Ubuntu	ALT Linux, CentOS, RHEL, Fedora, openSUSE



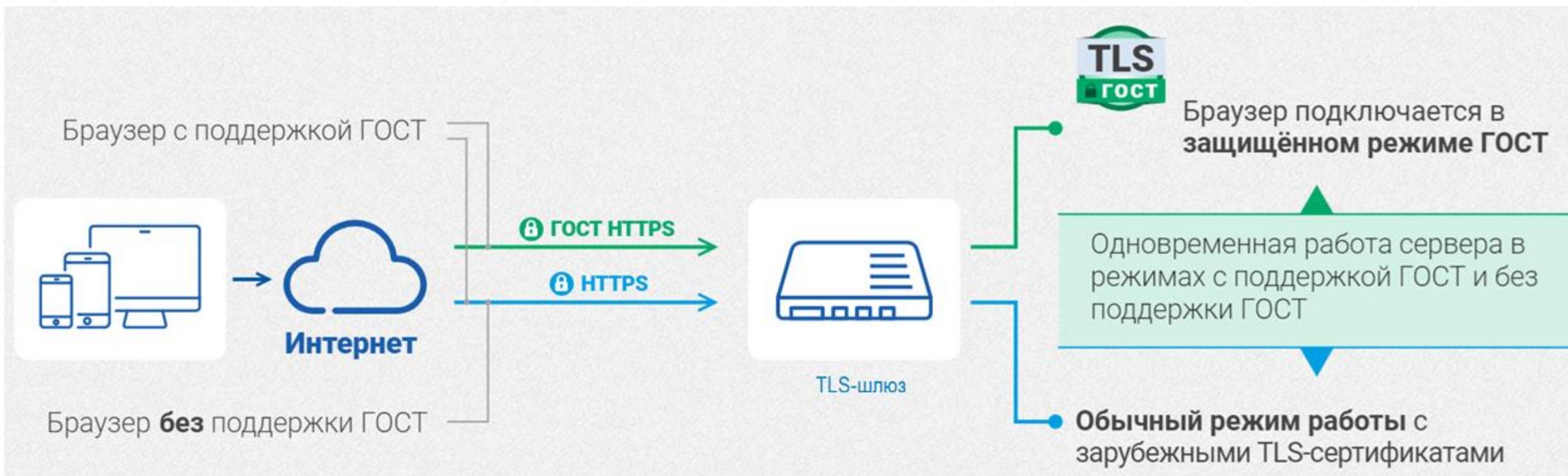

КриптоПро CSP и Яндекс.Браузер

Пакет программ поддерживает отечественное шифрование данных — протокол ГОСТ TLS. Его используют Госуслуги и некоторые другие сайты — например, на доменах gov.ru или nalog.ru

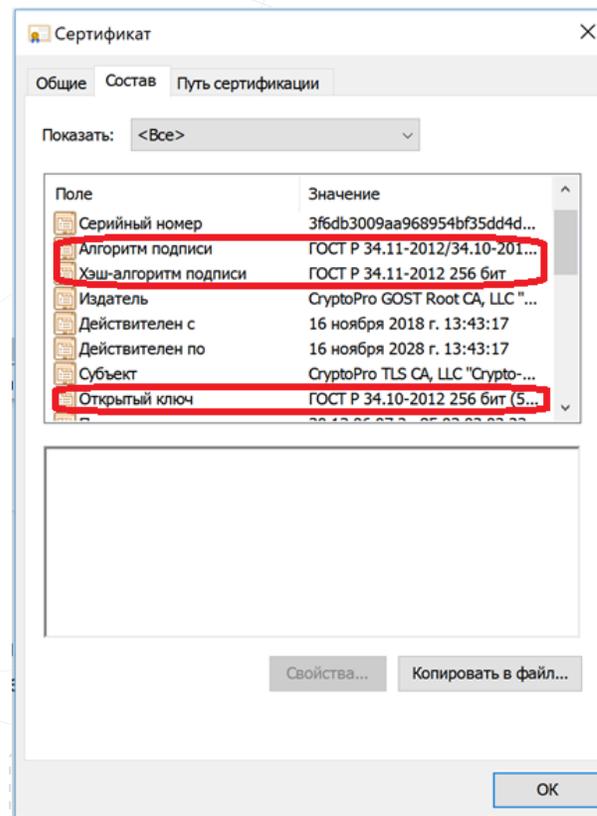
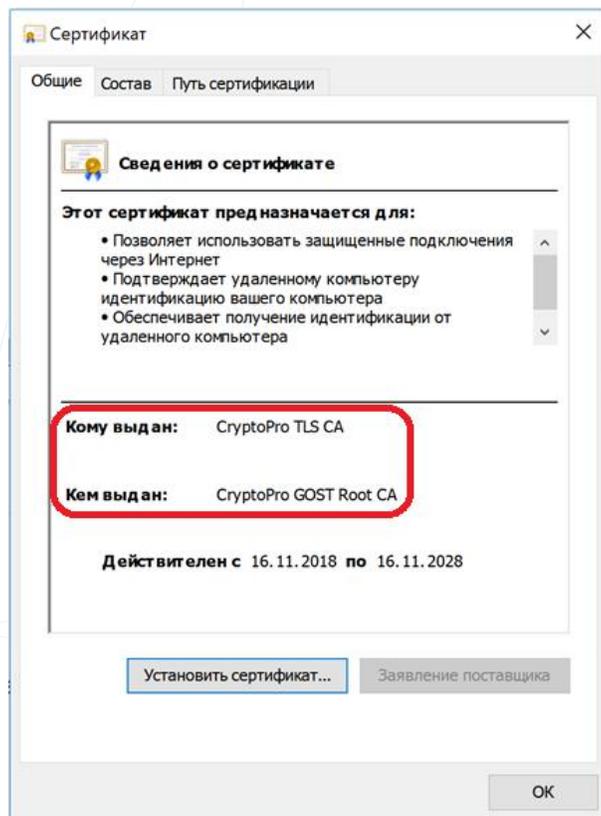


Протокол ГОСТ TLS

Протокол использует криптографические алгоритмы — в итоге между пользователем и сервером возникает защищённый канал связи. Он обеспечит высокую безопасность голосования

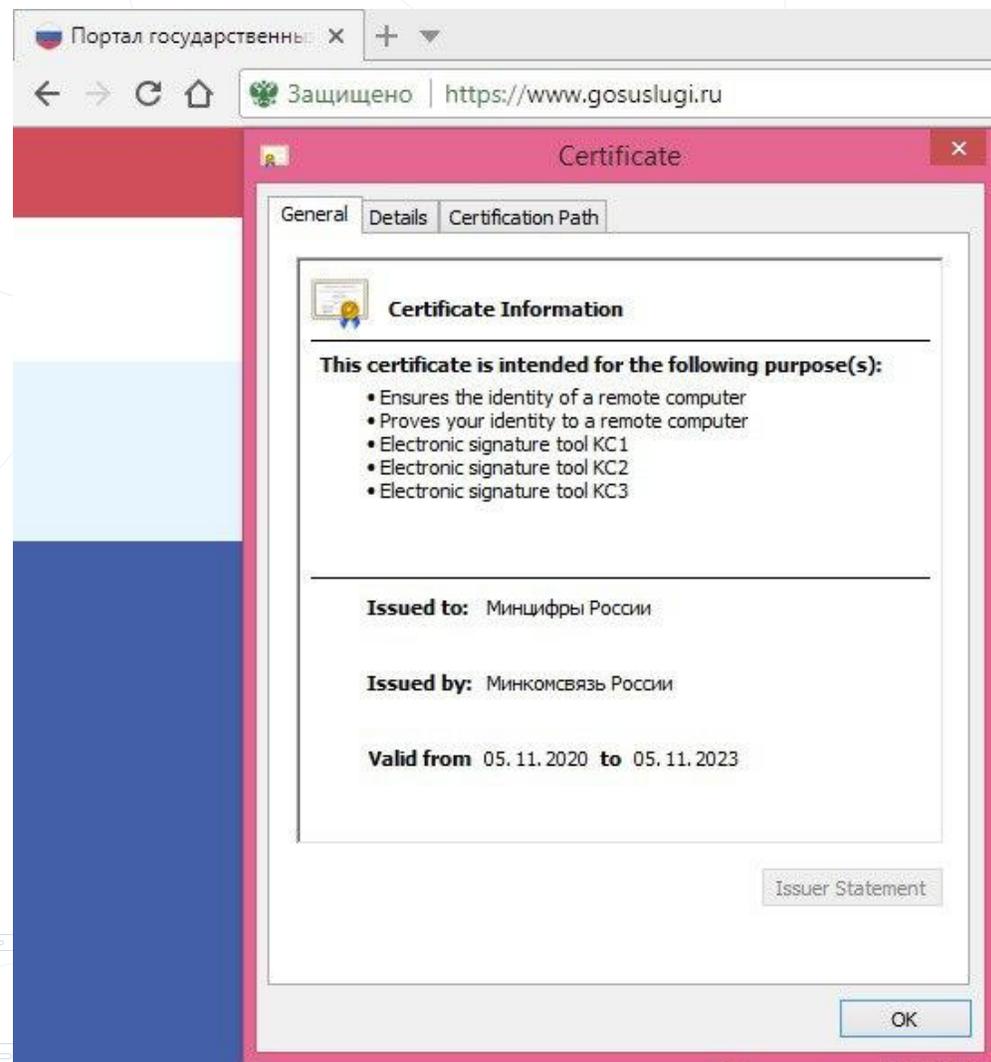


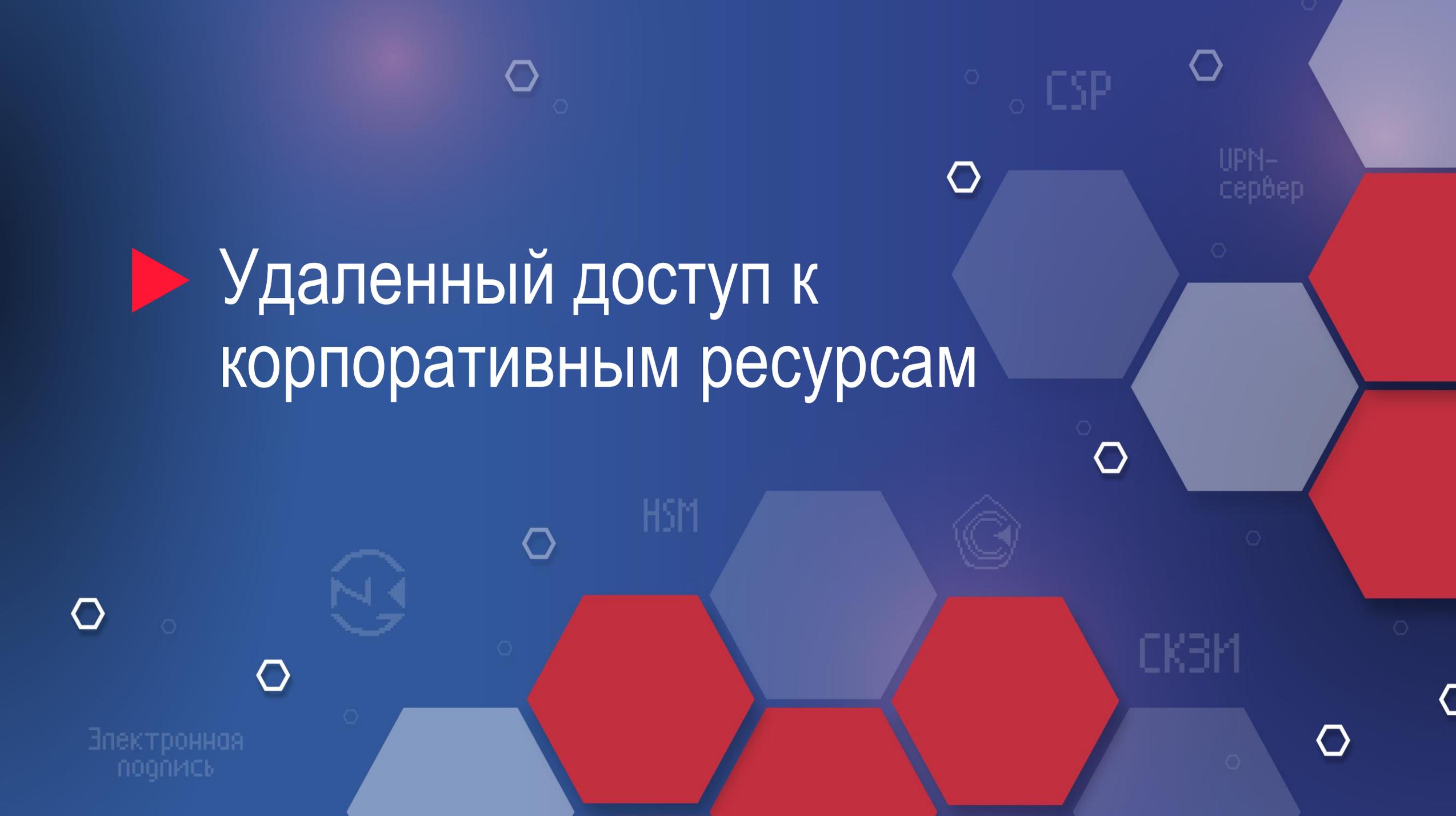
- Получить RSA-сертификат (в зарубежном УЦ и/или в НУЦ)
- Получить ГОСТ-сертификат
- Использовать на веб-сайте одновременно два сертификата – RSA и ГОСТ





- <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





▶ Удаленный доступ к
корпоративным ресурсам

Электронная
подпись

denis-19 23 июня в 17:34

Cisco решила полностью уйти из России и Беларуси

IT-инфраструктура*, Сетевые технологии*, Сетевое оборудование, IT-компании



СТРАНА

Вышли из строя: к чему приведет уход зарубежных вендоров из сферы кибербезопасности

Смогут ли российские компании заменить иностранных игроков

17 марта 2022, 16:00 | Олеся Тернопольская

IT-КОМПАНИИ | КИБЕРБЕЗОПАСНОСТЬ | ЛАБОРАТОРИЯ КАСПЕРСКОГО



Фото: ИЗВЕСТИЯ/Александр Казаков

denis-19 1 июля в 10:50

Производитель HSM-модулей Thales объявил об уходе из РФ

Информационная безопасность*, Сетевые технологии*, Финансы в IT, IT-компании



- Комплексное решение **NGate + SafeMobile + САКУРА** обеспечивает импортозамещение Cisco AnyConnect и возможность построения архитектуры **ZTNA** как с применением российской криптографии, так и зарубежной
- **САКУРА и SafeMobile** обеспечивают проверку подключающихся устройств на соответствие политикам ИБ
- **NGate** после проверки обеспечивает VPN-доступ пользователей к корпоративным ресурсам



На рынке отсутствует решение, способное в одиночку заменить Cisco AnyConnect*

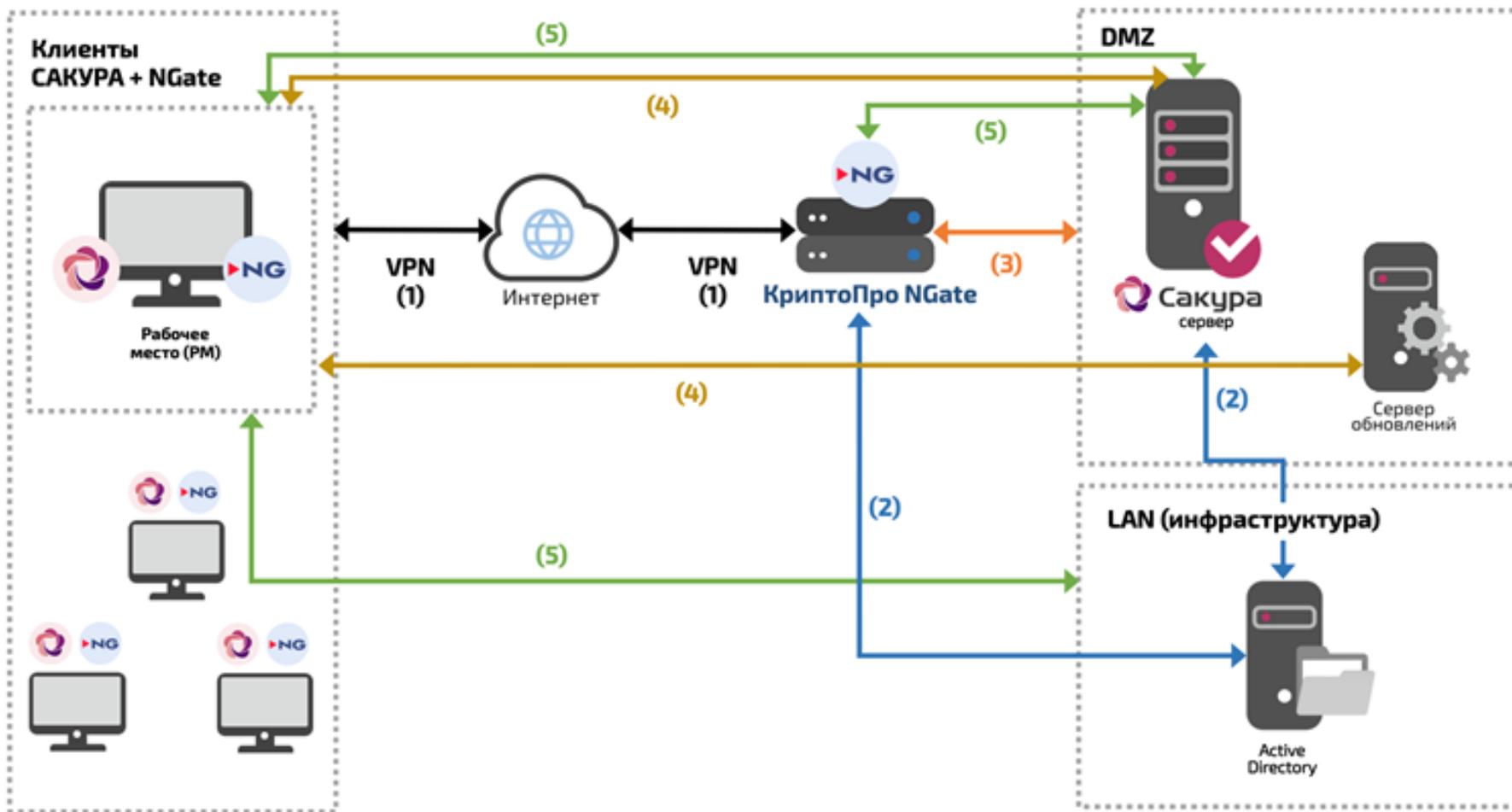
Примеры проверок:

- Проверка на взлом устройства, наличия антивируса
- Принадлежность устройства – корпоративное или личное
- Нахождение внутри или вне геозоны
- Доменные группы, в которых должен быть/не быть пользователь
- Наличие или отсутствие на устройстве заданных приложений
- Минимальная или максимальная версия мобильной ОС

Примеры реакций:

- Разрешение/запрет доступа по VPN
- E-mail по указанному шаблону
- Принудительное обновление ОС (для iOS);
- Установка compliance профиля





1. Клиентское рабочее место подключается по VPN к шлюзу NGate
2. Сервер САКУРА и шлюз NGate Синхронизируются с Active Directory (AD), где настроены группы доступа **COMPLIANT** и **NON-COMPLIANT**
3. По умолчанию, рабочее место находится в группе **NON-COMPLIANT**, имеющей доступ строго в DMZ, где расположены Сервер САКУРА и Сервер обновлений
4. Рабочее место проходит проверку на сервере САКУРА, по результатам пользователь перемещается в группу **COMPLIANT**, либо же клиенту САКУРА подается команда получить обновления компонентов с сервера обновлений
5. При успешном прохождении проверок PM, сервер САКУРА перемещает пользователя в группу **COMPLIANT**, шлюз NGate синхронизируется с AD и затем предоставляет доступ рабочему месту пользователя в инфраструктуру (LAN)

▶ КриптоПро NGate

Электронная
подпись

HSM

CSP

UPM-
сервер

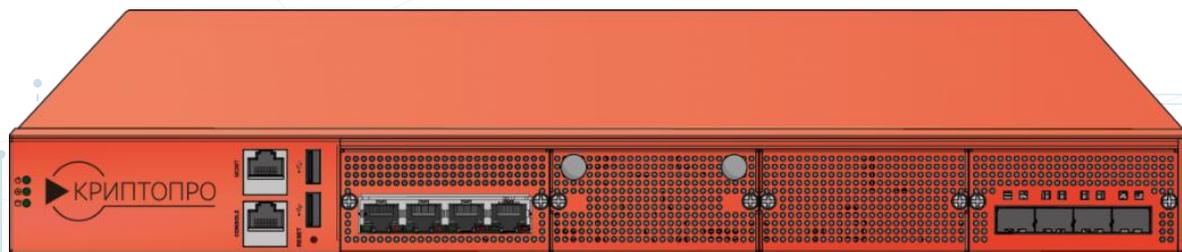
СКЭМ

КриптоПро NGate – универсальный криптографический шлюз, объединяющий в себе функционал:

- TLS-сервера доступа к веб-сайтам (**WEB TLS**)
- Сервера портального доступа (**WEB Portal TLS**)
- VPN-сервера удаленного доступа (**Point-to-Site TLS VPN**)
- VPN-сервера доступа между площадками (**Site-to-Site IPsec VPN**)



- Аппаратное и виртуальное исполнение (VMWare ESXi, KVM и т.д.)
- Производительность старшей модели **АП NGate 3000**:
 - ✓ В режиме **TLS-VPN**: **до 8 Гбит/с**
 - ✓ Количество одновременных аутентифицированных соединений: **12 000 шт.**
- Масштабирование посредством подключения в кластер новых узлов
- Полноценная кластеризация в режиме **Active-Active** с синхронизацией сессий





android 12



А В Р О Р А

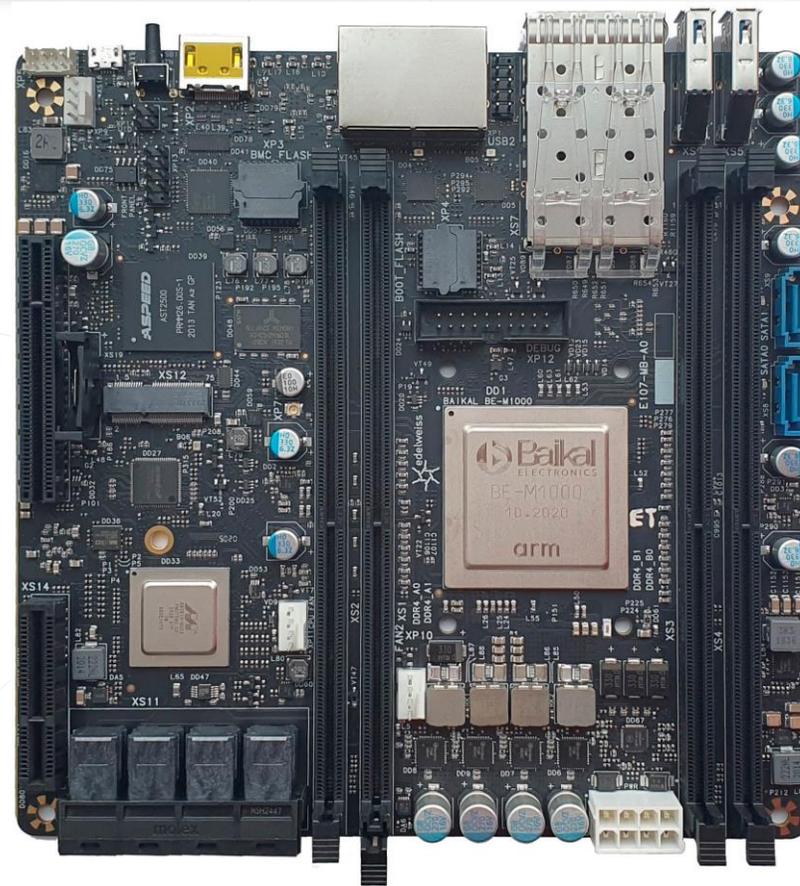
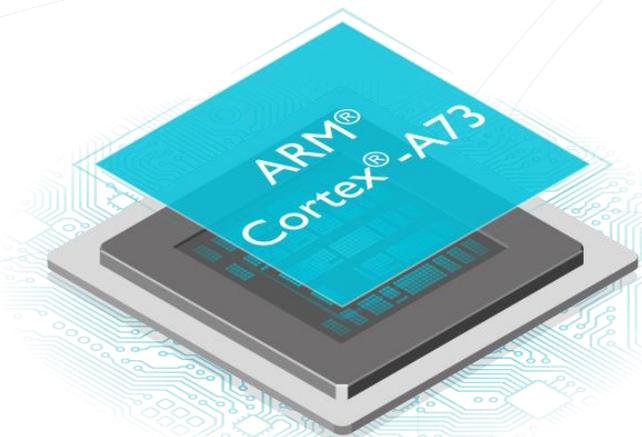


Windows 11



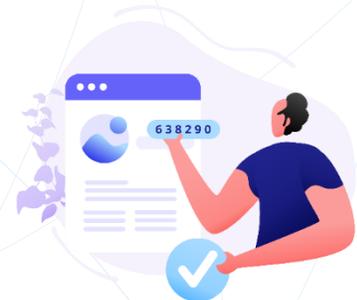
эльбрус





- Поддержка аутентификации по PSK и по сертификатам
- Удобное централизованное администрирование ключей PSK
- Вместо **client-to-site IPsec** реализован полноценный **TLS RA VPN**
- Встречная совместимость (ЭЛВИС-ПЛЮС, Криптонит, Фактор-ТС)
- NGate IPsec - это **IKEv2 + ESP**

- По логину/паролю (по группам в LDAP/AD)
- По клиентским сертификатам (в т.ч. по полям и OID)
- MFA (интеграция через RADIUS)
- Поддержка аппаратных ключей по USB/Bluetooth/NFC
- **Составные схемы аутентификации!**



- Поддержка ГОСТ и зарубежных алгоритмов
- Сертифицирован ФСБ России по классам КС1, КС2 и КС3
- Клиенты под все популярные ОС (в т.к. мобильные)
- Поддержка работы без клиента (через браузер)
- Контроль доступа на уровне веб-приложений
- Ограничение времени сессии пользователей
- Есть экспортный вариант



Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Суцьевский Вал, д.18

Тел./факс: +7 (495) 995-48-20

<https://cryptopro.ru>

Персональные вопросы: plutsik@cryptopro.ru

Общие вопросы: info@cryptopro.ru

Контрактный отдел: kpo@cryptopro.ru

Для дилеров: dealer@cryptopro.ru

