

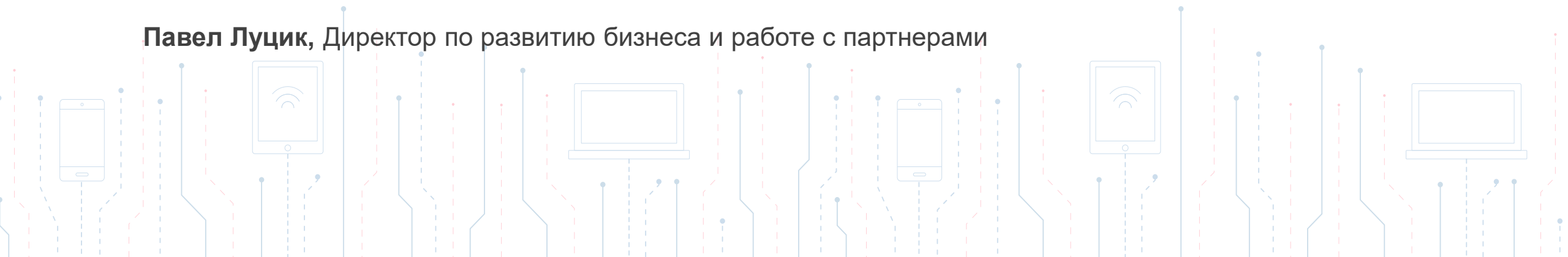


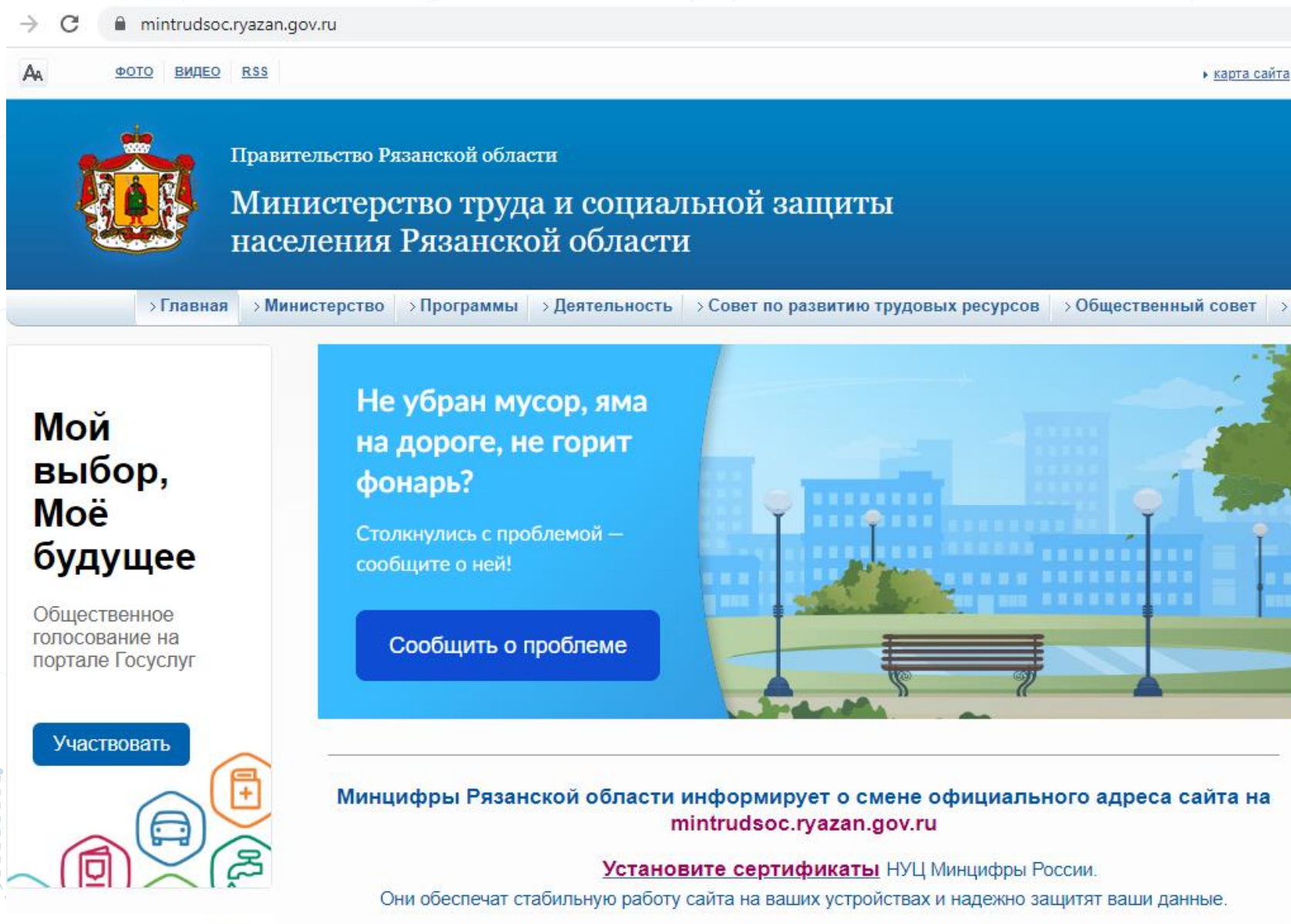
Ключевое слово
в защите информации



Импортозамещение средств защищенного удаленного доступа в условиях санкций


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

СКЗМ

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

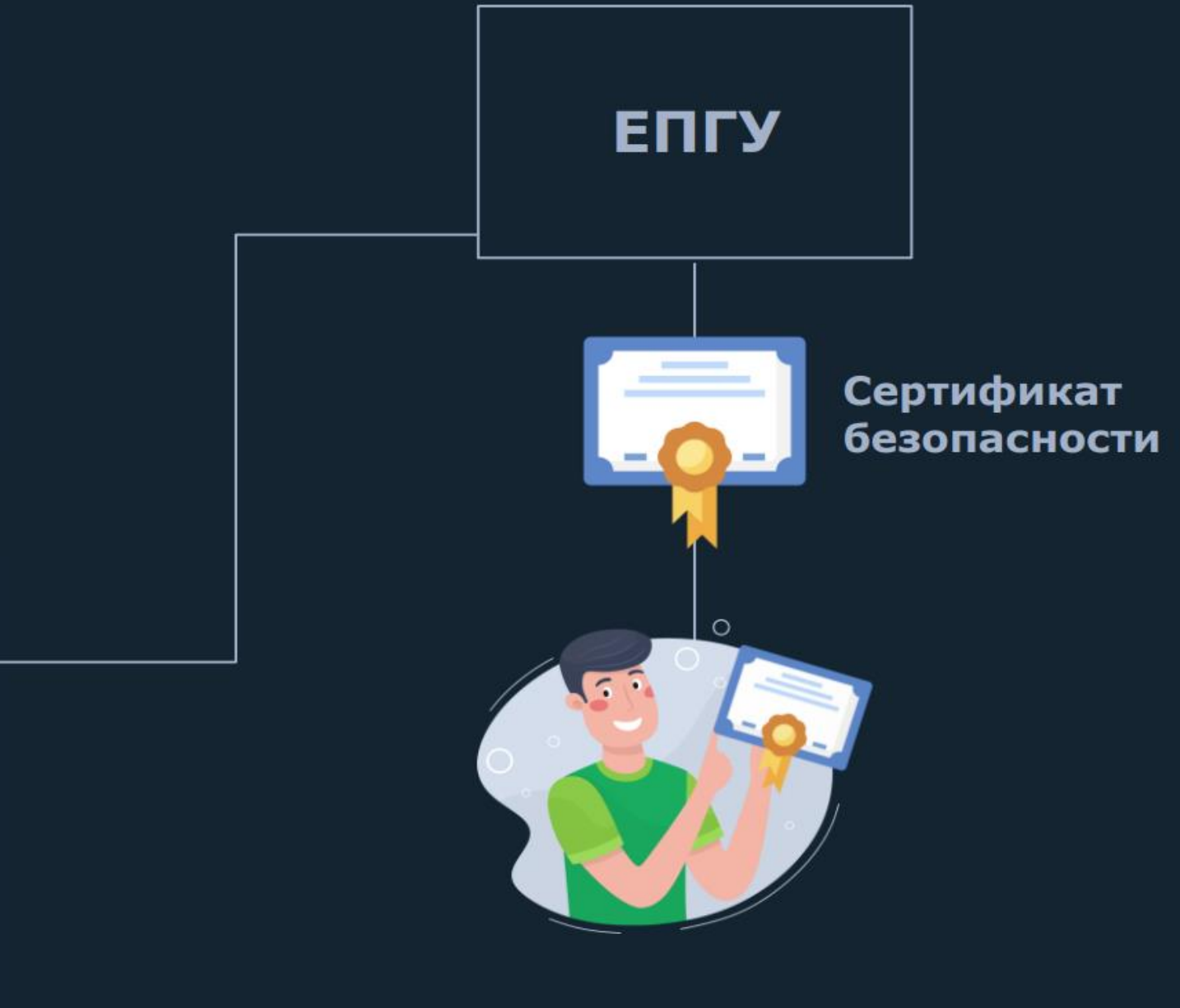
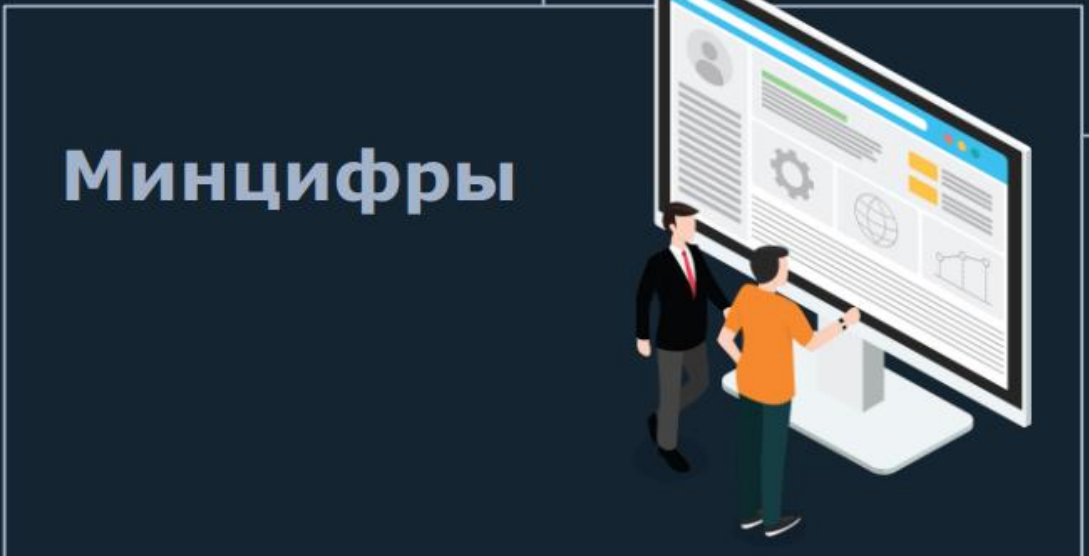
HSM

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

Скачать сертификат

Скачать CSV-файл

Скачать сертификат

Корневой сертификат удостоверяющего центра

<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	B	C
1012	www.partizansk.primorsky.ru		
1013	primorsky.ru		
1014	*.primorsky.ru		
1015	*.mil.ru		
1016	online.in-bank.ru		
1017	assist24.kubankredit.ru		
1018	and-up7-asbs.online.sberbank.ru		
1019	sovcomins.ru		
1020	pulse.sber.ru		
1021	sbnk.ru		
1022	friend.sbrf.ru		
1023	uat.sberxba.ru		
1024	egwtest.open.ru		
1025	*.energotransbank.com		
1026	sberkids-t.sberbank.ru		
1027	demo.rcg.agency		
1028	emb.ru		
1029	*.bsoinsur.online		
1030	wt.vektorpharm.ru		
1031	db.sokbank.ru		
1032	ibank-1827.finsb.ru		
1033	join.kubankredit.ru		
1034	mobile.open.ru		

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 СБЕРБАНК

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 информации.

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](#)



[НОВОСТИ](#)

[АНОНСЫ](#)

[ПИСЬМО АДМИНИСТРАТОРУ](#)

[Карта сайта](#) | [Видеоматериалы](#)



Правительство Рязанской области

Министерство цифрового развития, информационных технологий и связи Рязанской области

[> Главная](#)

[> Министерство](#)

[> Направления](#)

[> Деятельность](#)

[> Документы](#)

ОБЪЯСНЯЕМ.РФ



**> ОТВЕТЫ
НА ВОПРОСЫ,
КОТОРЫЕ ВОЛНУЮТ ВСЕХ**

УЗНАЙ ПРЯМО СЕЙЧАС



Проблемы с госуслугами, медленный интернет или плохая связь?

Напишите об этом — Минцифры поможет с решением

**Минцифры Рязанской области информирует о смене
официального адреса сайта на it.ryazan.gov.ru**

Установите сертификаты НУЦ Минцифры России. Они обеспечат стабильную работу сайта на ваших устройствах и надежно защитят ваши данные.

**Геоинформационная
система
Рязанской области**

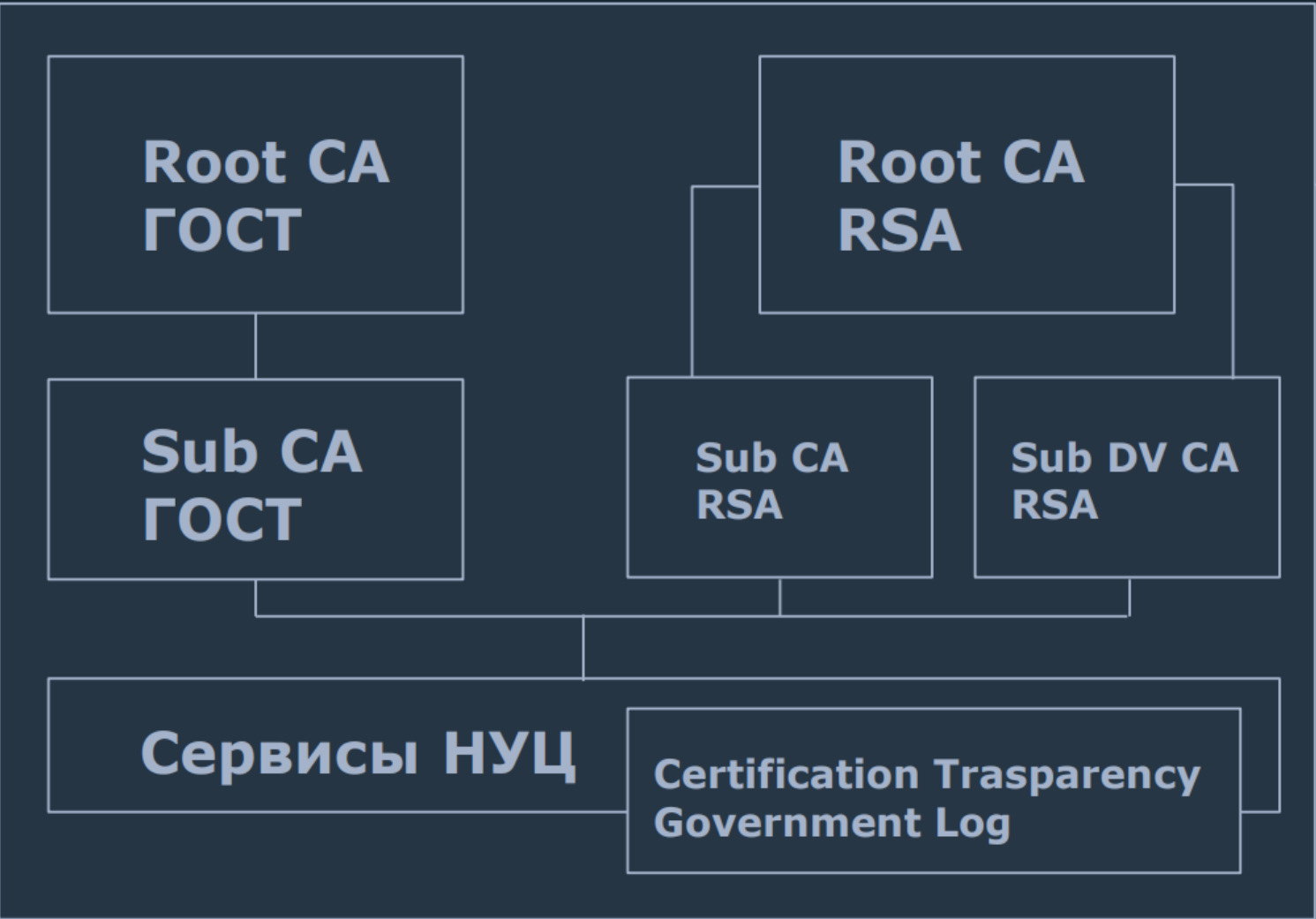


SSL/TLS с RSA

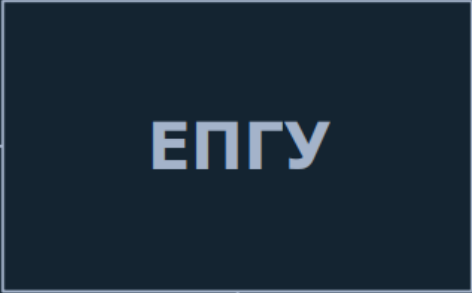
- RFC
- Поддержка со стороны браузеров
- Удостоверяющие центры
- Серверные решения (шлюзы)
- Массовость

TLS с ГОСТ

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



Certification Transparency Log



Сертификат безопасности



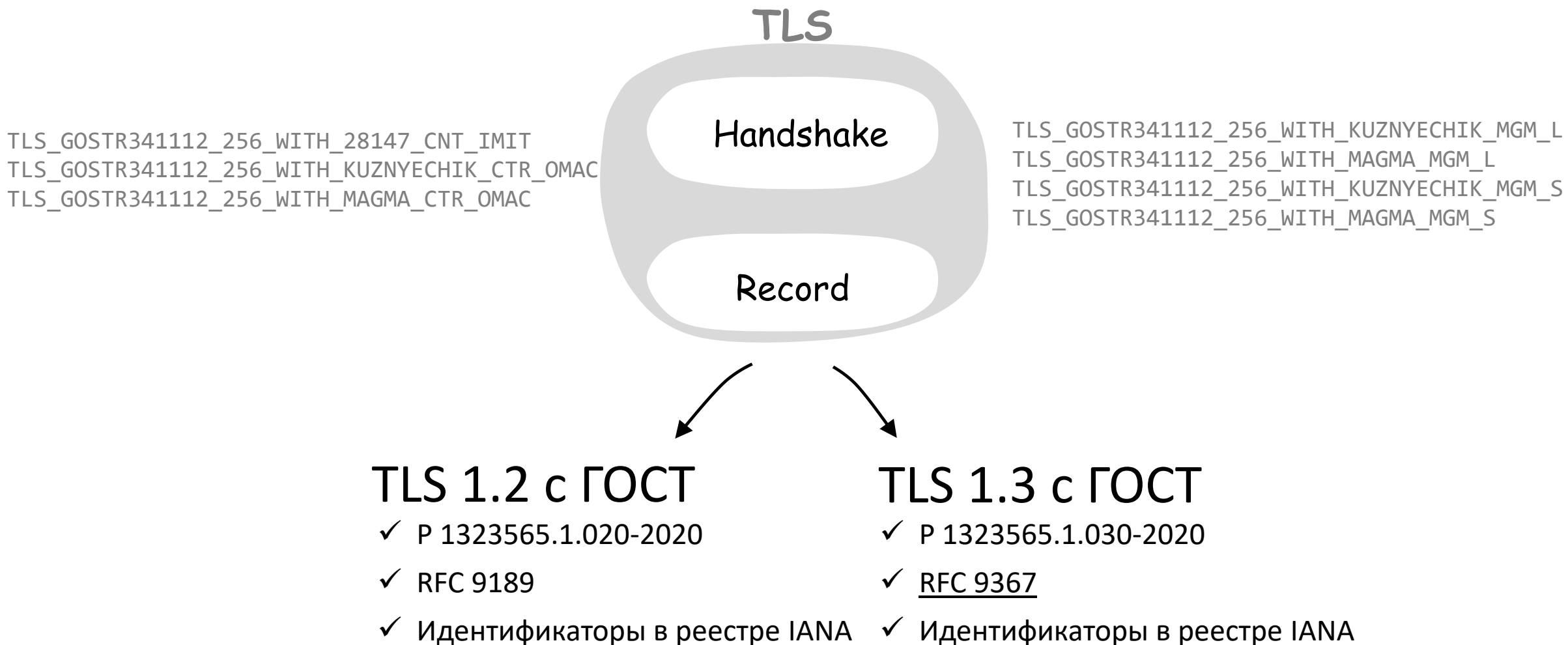
Получение сертификата ГОСТ TLS

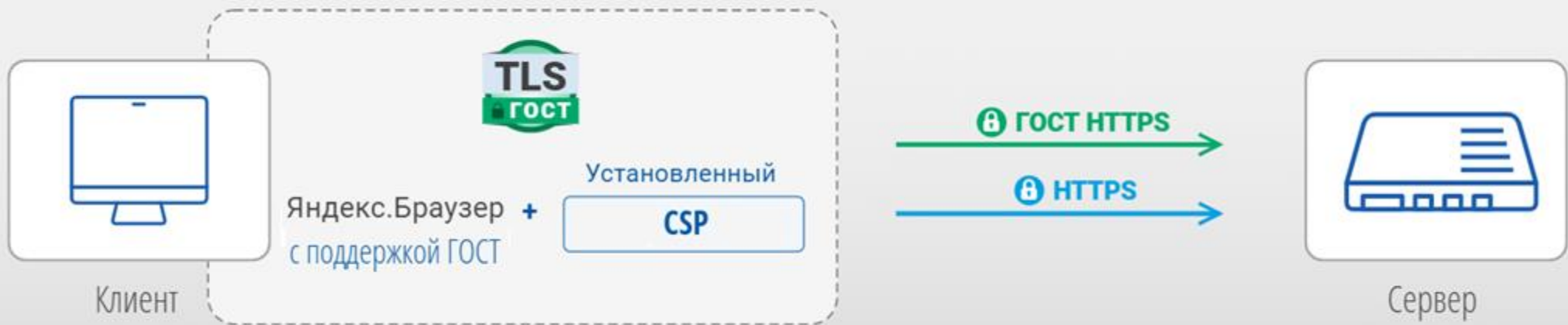
Удостоверяющего центра CryptoPro TLS CA



Удостоверяющий центр
CryptoPro TLS CA



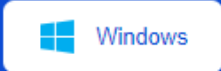




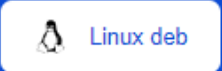
The screenshot shows the website gosuslugi.ru/browser. The browser address bar contains 'gosuslugi.ru/browser'. The page header includes the 'gosuslugi' logo with 'Москва' next to it, and navigation links for 'Помощь', 'Войти', and 'Регистрация'. The main content area has a blue background with the title 'Пакет программ для безопасного голосования'. Below the title is a paragraph: 'Скачайте браузер с шифрованием данных по ГОСТ TLS. Для Windows уже включён КриптоПро CSP. Для Linux КриптоПро нужно [скачать отдельно](#)'. There are three buttons for operating systems: 'Windows' (already included), 'Linux deb' (Astra Linux, Debian, Ubuntu), and 'Linux rpm' (ALT Linux, CentOS, RHEL, Fedora, openSUSE). An illustration shows a person pointing at a large screen displaying a ballot box. Below this are two white boxes: 'КриптоПро CSP и Яндекс.Браузер' and 'Протокол ГОСТ TLS', each with an icon and descriptive text.

Пакет программ для безопасного голосования

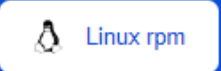
Скачайте браузер с шифрованием данных по ГОСТ TLS.
Для Windows уже включён КриптоПро CSP.
Для Linux КриптоПро нужно [скачать отдельно](#)



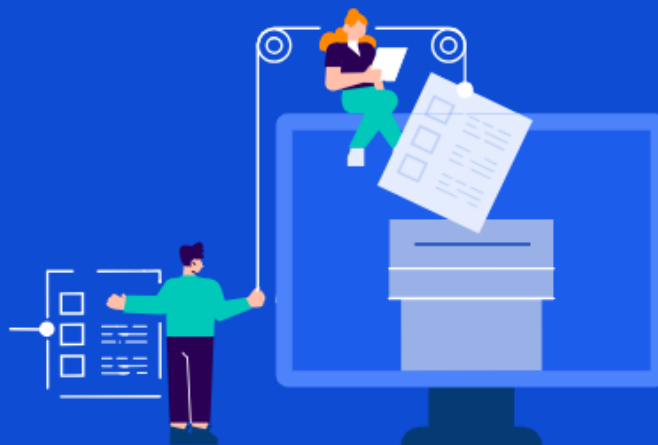
Уже включён
КриптоПро CSP



Astra Linux,
Debian, Ubuntu



ALT Linux, CentOS, RHEL,
Fedora, openSUSE



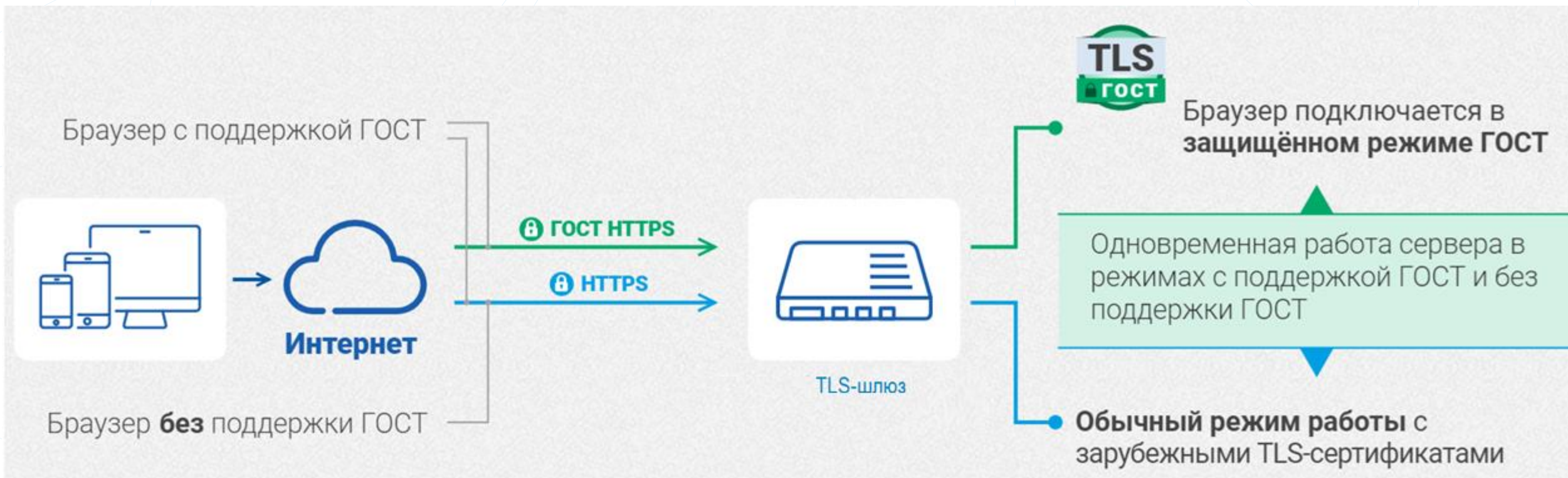
КриптоПро CSP и Яндекс.Браузер

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

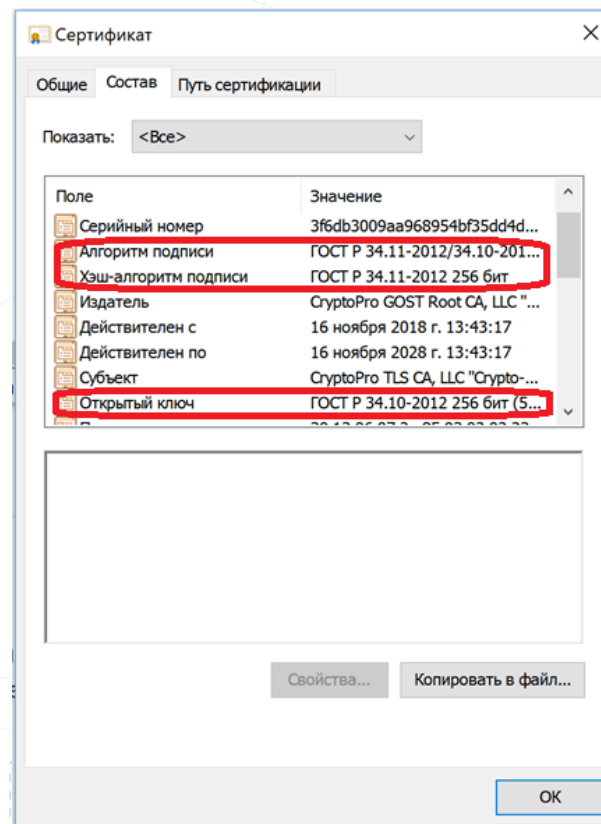
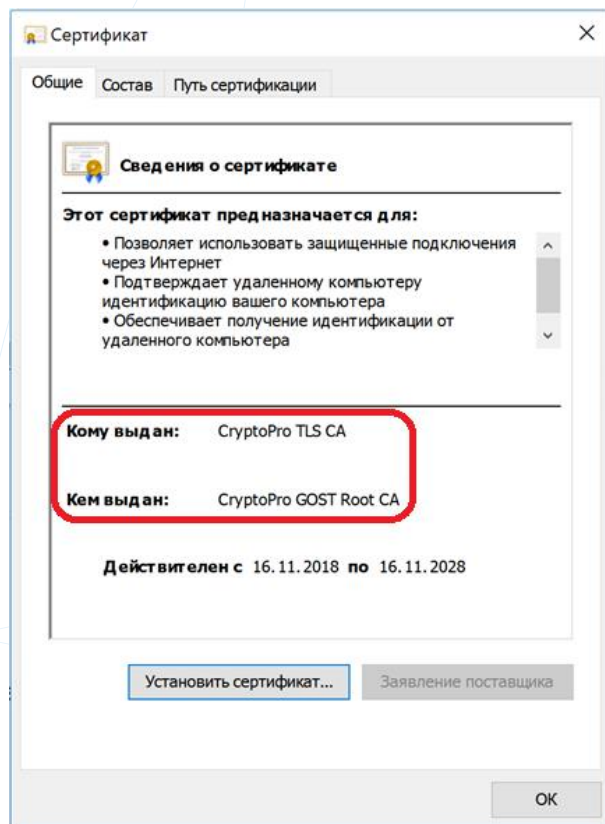


Протокол ГОСТ TLS

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

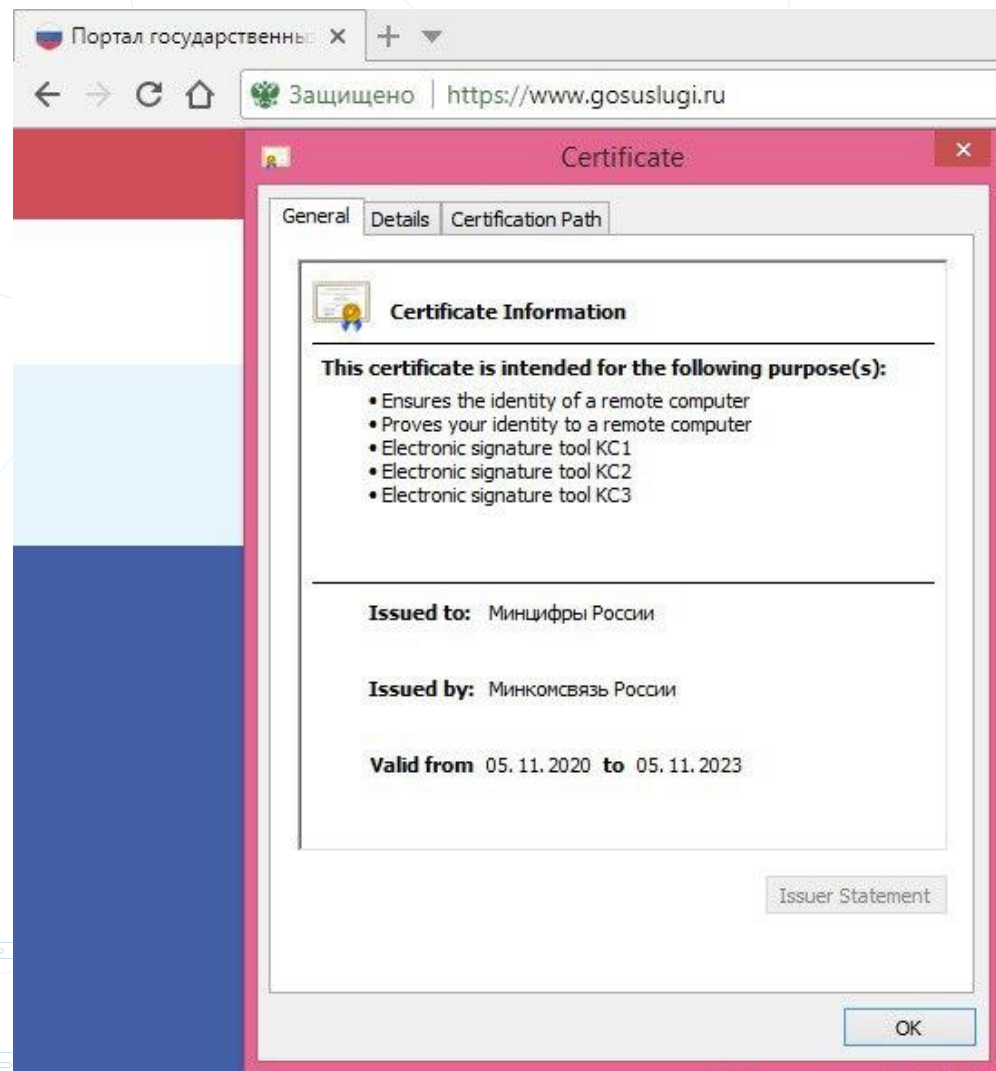


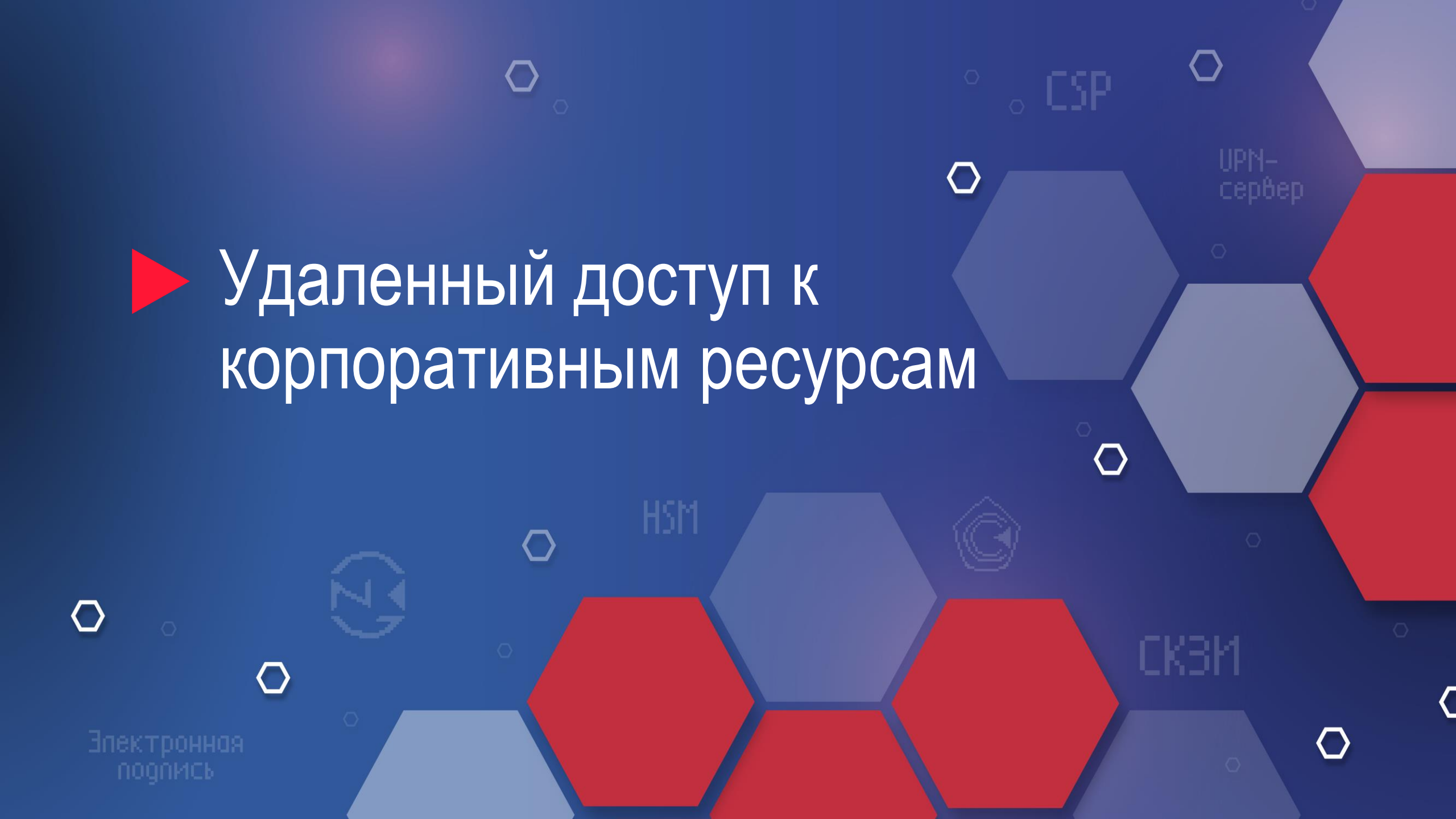
- Получить RSA-сертификат (в зарубежном УЦ и/или в НУЦ)
- Получить ГОСТ-сертификат
- Использовать на веб-сайте одновременно два сертификата – RSA и ГОСТ





- <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

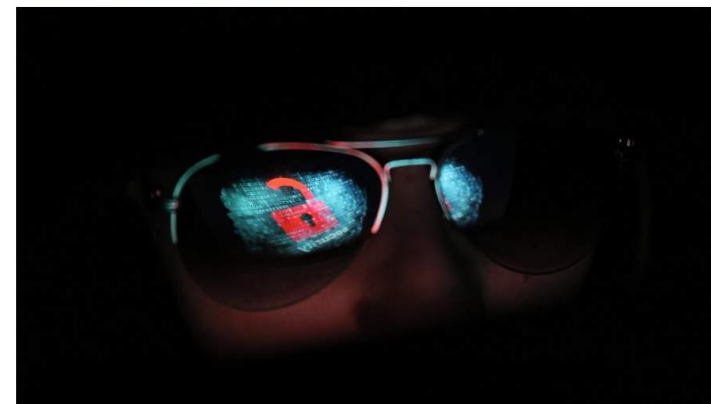


Фото: ИЗВЕСТИЯ/Александр Казаков

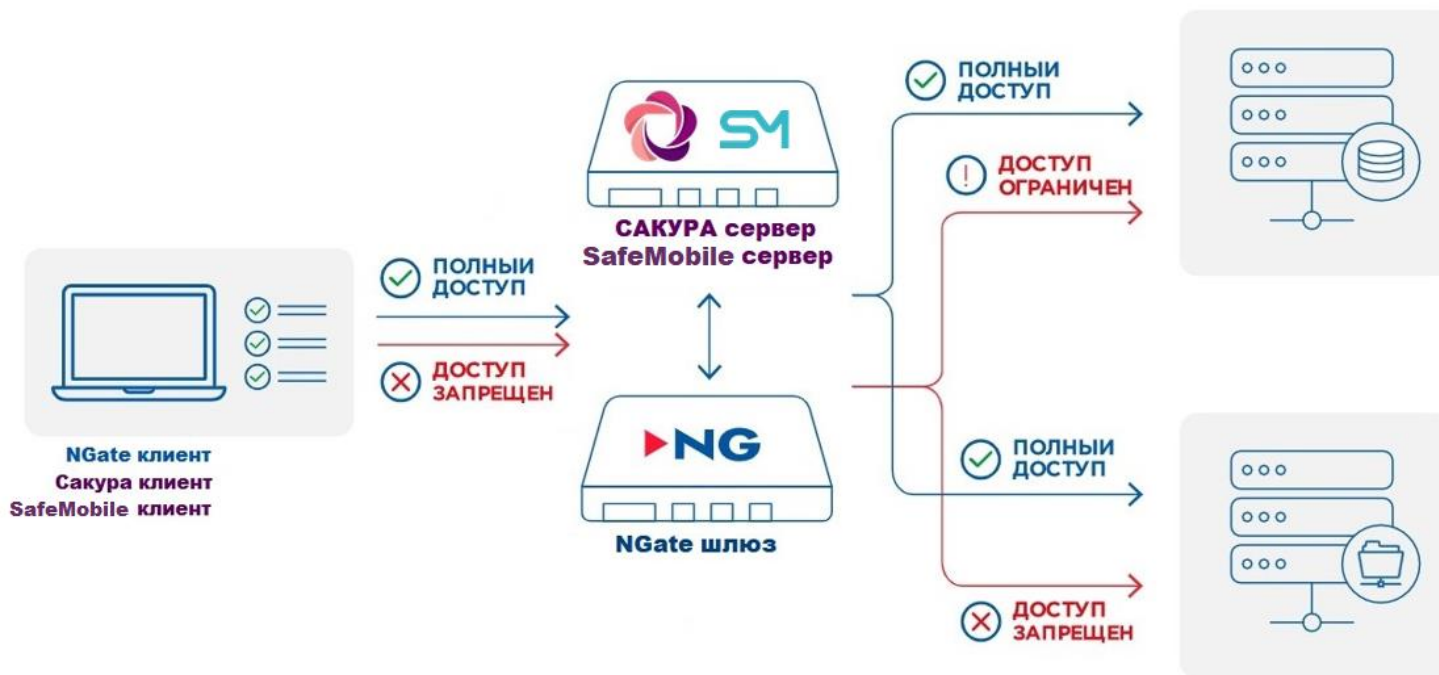
denis-19 1 июля в 10:50

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*

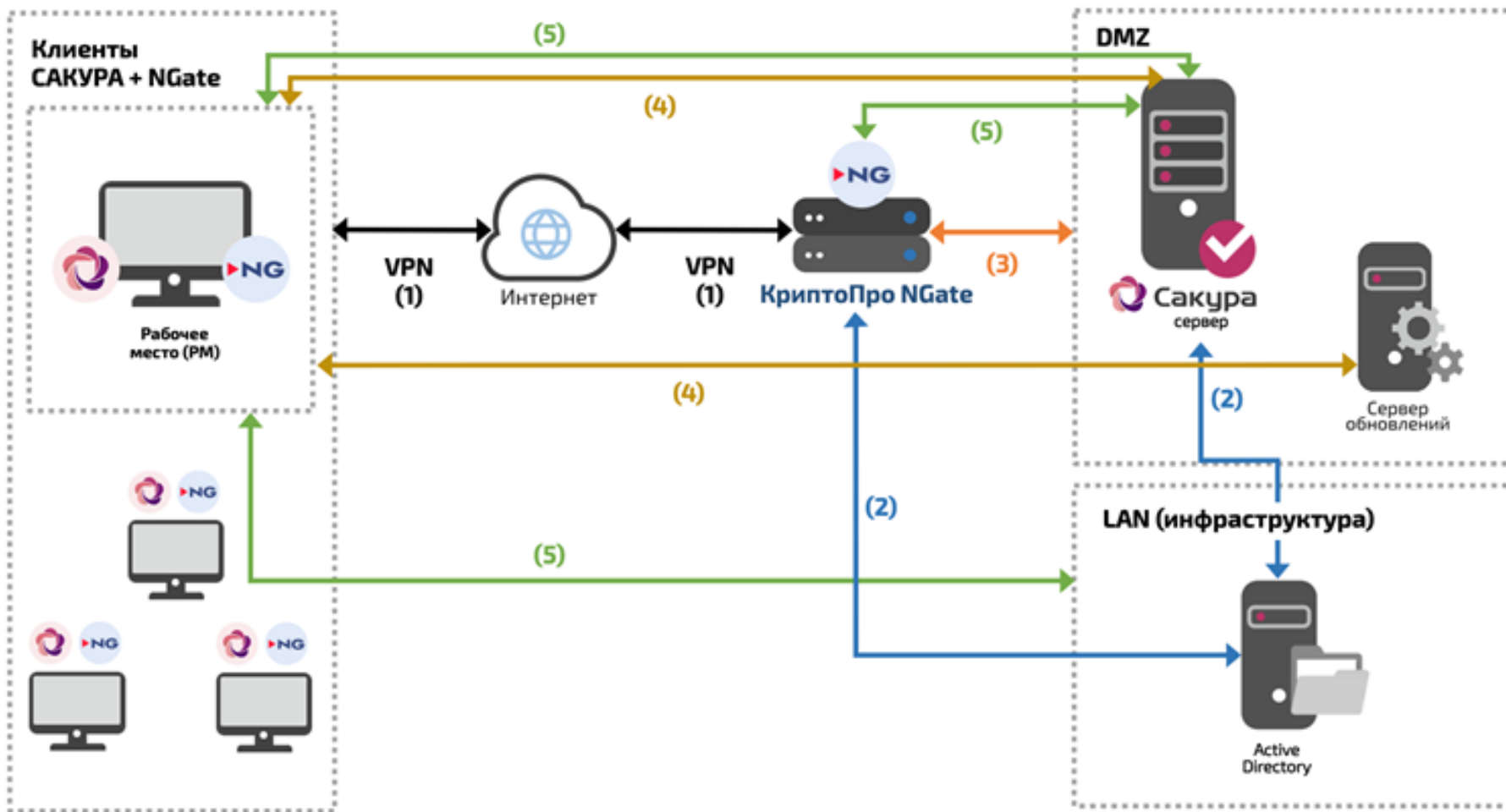
Примеры проверок:

- 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

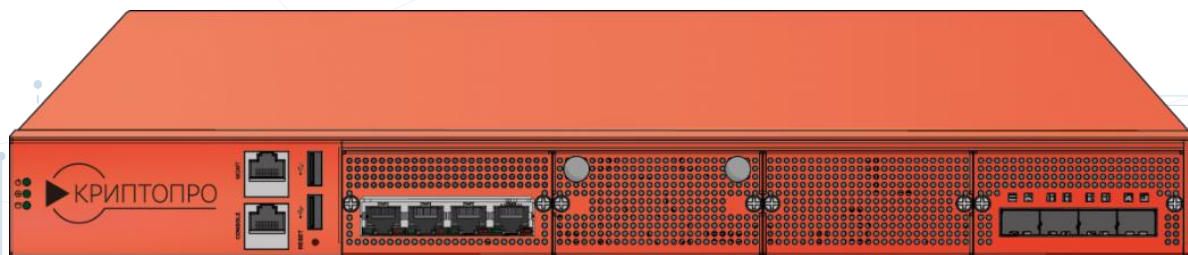
СКЗМ

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

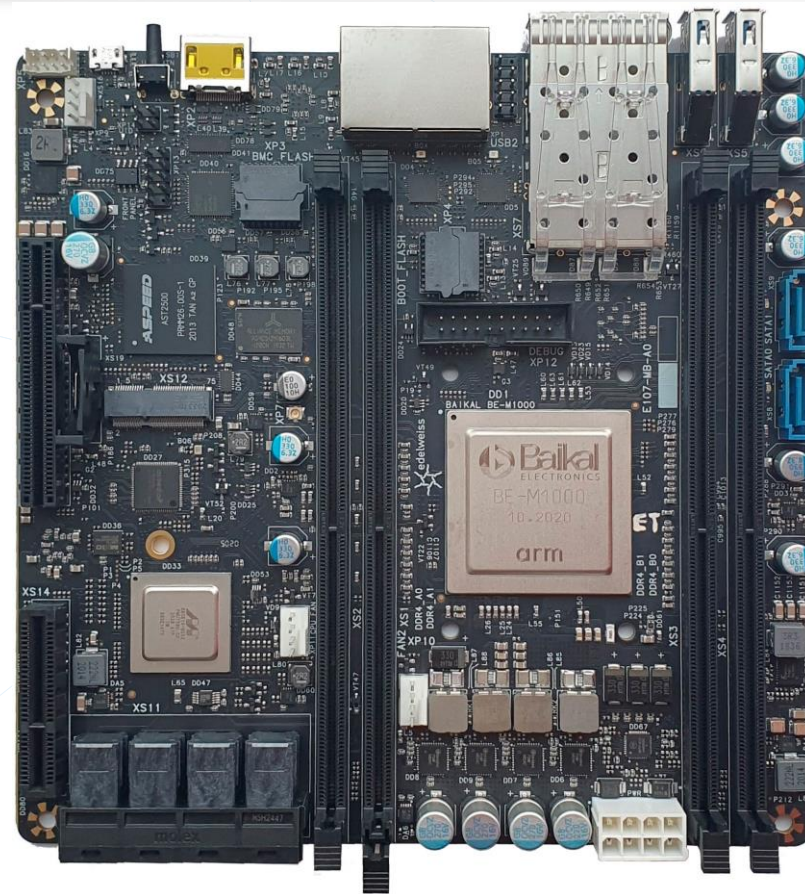
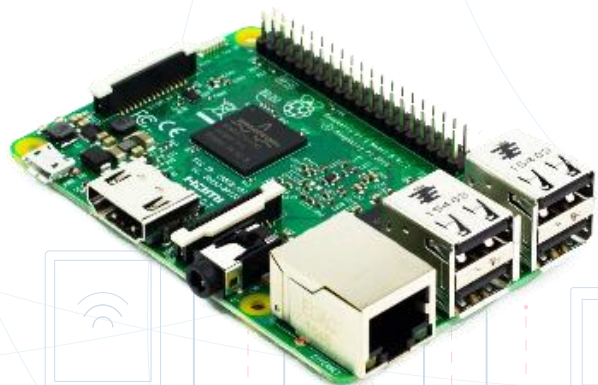
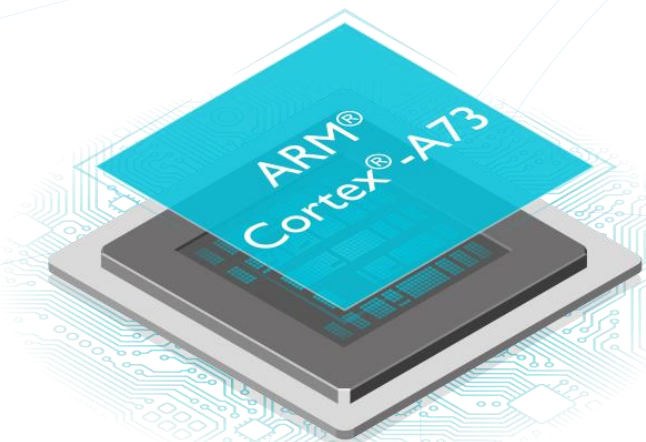


Windows 11



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

26 июня 2023 14:35 | 👁 3325 | ➦ ПОДЕЛИТЬСЯ

CNews FORUM
1 ноября

CNews AWARDS
1 ноября

Бизнес-коммуникации

Импортозамещение

Безопасность

ИТ в госсекторе

ИТ в банках

ИТ в торговле

Цифровизация

Телеком

Создан первый российский аппаратный модуль для безопасных платежей на замену европейским аналогам

«Криптопро» получила все необходимые разрешительные документы для распространения аппаратных модулей безопасности собственной разработки. Эти устройства работают в банках и обеспечивают защиту транзакций от хакеров. Они создавались на замену модулей французской Thales – крупнейшего вендора таких устройств, ушедшего из России в 2022 г. Новинка «Криптопро» – первый модуль, у которого есть все необходимые сертификаты. Он уже тестируется в банках, но назвать его на 100% отечественным нельзя – в нем немало иностранных компонентов.



29 июня 2023 09:10 | [ПОДЕЛИТЬСЯ](#)**CNews FORUM**
1 ноября**CNews AWARDS**
1 ноября

Бизнес-коммуникации

Импортозамещение

Безопасность

ИТ в госсекторе

ИТ в банках

«КриптоПро Ключ» – новое слово в безопасности мобильной подписи

Компания «КриптоПро» объявляет о разработке принципиально нового комплексного продукта для мобильной подписи – «КриптоПро Ключ», мобильных SDK и мобильных приложений на их основе.

Разработка ведется по **техническому заданию**, согласованному в мае 2023 г. с ФСБ России. Среди различных вариантов использования «**КриптоПро Ключа**» доступен инновационный способ защиты ключей подписи. Их безопасность при хранении в мобильных устройствах обеспечивается с помощью ключей защиты, которые находятся на серверной стороне в HSM в неизвлекаемом виде.





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

