## Установка корневого сертификата Российского Национального Удостоверяющего Центра на компьютер под операционной системой Windows 10/11

Сертификаты безопасности предназначены для аутентификации сайтов в интернете при установлении защищенного соединения к ним, а также для безопасной работы мобильных приложений на смартфонах. Они обеспечивают передачу данных в зашифрованном виде, подтверждают подлинность сайтов, защищают онлайн-транзакции.

В ближайшее время сертификаты, выпущенные международными компаниями (Удостоверяющими Центрами - УЦ), будут заменяться на сертификаты, выпущенные Российским Национальным УЦ (МинЦифра). Для обеспечения возможности работы зарубежных браузеров (Google Chrome/Chromium, Mozilla FireFox, Opera, Edge) и смартфонов (операционные системы Android и iOS) с ресурсами, защищёнными с помощью российских сертификатов, <u>необходима загрузка и установка корневого сертификата</u> **Российского Национального УЦ** на компьютеры и устройства.

В случае использования российских браузеров Яндекс.Браузер или Atom описываемая ниже загрузка и установка не обязательны (поддержка корневого сертификата Российского Национального УЦ в них встроена).

- 1. Перейти на сайт по ссылке <u>https://www.gosuslugi.ru/tls</u>
- 2. На открывшейся странице выбрать раздел «Корневой сертификат удостоверяющего центра» и нажать на кнопку «Скачать сертификат»:

<b>≡ госуслуги</b>	Климовск г	Помощь Q	Войти Регистрация
	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 интернет защищенного соединения. Помогает передавать данные в зашифрованном ви подлинность сайта и его принадлежность владельцу, защищает онлайн Получить сертификат Спифок доменов, в отношении которых выпущены сертификаты безо Скачать CSV-файл Корневой сертификат удостоверяющего центра Качать сертификат	те при установлении иде, подтверждать н-транзакции	

3. После загрузки необходимо открыть загруженный файл «RootCa\_SSL\_RSA.zip»:



4. В появившемся окне необходимо выбрать файл со значком подписи:



5. Согласиться с предложением на открытие файла нажав на кнопку «Открыть»:



6. Откроется окно, позволяющее установить сертификат. Выберите в этом окне кнопку «Установить сертификат...»:

🖬 Сертификат 🛛 🗙	$\langle  $
Общие Состав Путь сертификации	
Сведения о сертификате	
Этот сертификат предназначается 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 23.02.2032	
k	
Установить сертификат Заявление поставщика	
ОК	

7. В окне «Мастер импорта сертификатов» убедитесь, что выбран пункт «Текущий пользователь» и нажмите кнопку «Далее»:

🗧 😺 Мастер импорта сертификатов	×
Мастер импорта сертификатов	
Этот настер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.	
Расположение хранилища	
Для продолжения нажните кнопку "Далее".	
Далее Отмен	a

8. Выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите «Обзор...»

Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную. Автоматически выбрать хранилище на основе типа сертификата
Опроветить все сертификаты в следующее хранилище Хранилище сертификатов: Обзор

9. В окне «Выбор хранилища сертификата» выберите пункт «Доверенные корневые центы сертификации» и нажмите «ОК»

Выбор х	ранилища сертифик	сата	×
Выберит хотите и	е <u>х</u> ранилище сертифи спользовать.	катов, которое в	зы
· ····	Личное		^
	Доверенные корневы	е центры сертис	
Доверенные корневые центры сертиф Доверительные отношения в предпри Промежуточные центры сертификаци			
	Промежуточные цент	ры сертификаци	
	Доверенные издател	и	<b>v</b>
<	Септификаты к кото	оым нет доверик	
Оказ	ать физические хран	илища	
	ОК	Отмена	

10.Убедитесь, что выбран пункт «Поместить все сертификаты в следующее хранилище» и Хранилище сертификатов указано «Доверенные корневые центры сертификации» и нажмите кнопку «Далее»

Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную. ○ <u>А</u> втоматически выбрать хранилище на основе типа сертификата © <u>П</u> оместить все сертификаты в следующее хранилище Хранилище сертификатов: Доверенные корневые центры сертификации
Далее Отмена

11.Подтверждаем импорт сертификата нажав на кнопку «Готово»:

одержимое Сертификат	Сертификат

12. При появлении Предупреждения системы безопасности согласиться с установкой сертификата и нажать кнопку «Да»:

Предупреждение системы безопасности     ×       Image: Comparison of the comparation of the the the comparation of the			
Урадат установлен сертификат от центра сертификации (ЦС), представляющий:       Russian Trusted Root CA       Windows не удается проверить, что сертификат действительно получен от "Russian Trusted Root CA".       Обратитесь к "Russian Trusted Root CA" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:       Отпечаток (sha1): 8FF915CC AB7BC16F 8C5C8099 D53E0E11 SB3AEC2F       Предупреждение:       Кли вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.       Вы хотите установить этот сертификат?	Предупр	еждение системы безопасности	×
Russian Trusted Root CA     Windows не удается проверить, что сертификат действительно получен от "Russian Trusted Root CA". Обратитесь к "Russian Trusted Root CA" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:     Orneчаток (sha1): 8FF915CC AB7BC16F 8C5C8099 D53E0E11 SB3AEC2F     Предупреждение:     Коли вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификат, Budanhomy этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.     Вы хотите установить этот сертификат?		Будет установлен сертификат от центра сертификации (ЦС), представляющий:	
Windows не удается проверить, что сертификат действительно получен от "Russian Trusted Root CA".     Обратитесь к "Russian Trusted Root CA" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:     Отпечаток (sha1) : 8FF915CC AB7BC16F 8C5C8099 D53E0E11 SB3AEC2F     Предупреждение:     Если вы установите этот корневой сертификат, Windows 6удет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.     Вы хотите установить этот сертификат?		Russian Trusted Root CA	
Отпечаток (sha1) : 8FF915CC AB7BC16F 8C5C8099 D53E0E11 5B3AEC2F Предупреждение: Если вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск. Вы хотите установить этот сертификат? <u>Да</u> <u>Н</u> ет		Windows не удается проверить, что сертификат действительно получен от "Russian Trusted Root CA". Обратитесь к "Russian Trusted Root CA" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:	
Предупреждение: Если вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск. Вы хотите установить этот сертификат? <u>Д</u> а <u>Н</u> ет		Отпечаток (sha1): 8FF915CC AB7BC16F 8C5C8099 D53E0E11 5B3AEC2F	
Вы хотите установить этот сертификат? <u>Д</u> а <u>Н</u> ет		Предупреждение: Если вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.	
<u>Д</u> а <u>Н</u> ет		Вы хотите установить этот сертификат?	
		<u>Д</u> а <u>Н</u> ет	

13.В результате успешного импорта у Вас на экране появится подтверждающий диалог:



14.Загрузка Сертификата в хранилище сертификатов безопасности закончена.

## Проверка наличия корневого сертификата Российского Национального Удостоверяющего Центра, установленного на компьютер под операционной системой Windows 10/11

1. Запустите браузер MS Edge / Internet Explorer



2. В правом верхнем углу открывшегося браузера нажмите на троеточие/значок с шестеренкой:



3. В открывшемся меню выберите пункт меню Настройки/Свойства браузера:



4. В появившемся меню «Параметры» встаньте на поле поиска и начните набирать слово «сертификат», либо перейдите на закладку Содержание и нажмите кнопку Сертификаты. В итоге справа появится раздел «Управление сертификатами». Нажмите на появившийся раздел:

Параметры	Безопасность Управление параметрами безопасности в Microsoft Edge
🕲 Профили	Управление сертификатами
Конфиденциальность, поиск и службы	Управление сертификатами и настройками HTTPS/SSL
<li>Внешний вид</li>	Фильтр SmartScreen в Microsoft Defender Защитить устройство от вредоносных сайтов и загрузок с помощью фильтра Sma
🔄 Пуск, главная и новые вкладки	
Общий доступ, копирование и остория.	Блокировка потенциально нежелательных приложений Блокируется загрузка приложений с плохой репутацией, которые могут привести

5. Откроется окно «Сертификаты». Вам нужно выбрать вкладку «Доверенные корневые центры сертификации». Прокрутите список доступных сертификатов и убедитесь, что среди них присутствует сертификат под названием «Russian Trusted Root CA»:

			The second s	•
оверенные корневые цег	пры сертификации дов	еренные изда	тели издатели, не	
Кому выдан	Кем выдан	Срок де	Понятное имя	^
RootCA	RootCA	08.07.2023	<нет>	
ROOTsvc-CA	ROOTsvc-CA	07.08.2037	<нет>	
ROOTsvc-CA-test	ROOTsvc-CA-test	05.05.2035	<нет>	
ROOTsvc-CA-test	ROOTsvc-CA-test	04.05.2037	<het></het>	
Russian Trusted Ro	Russian Trusted Root	28.02.2032	<нет>	
Security Communic	Security Communicati	29.05.2029	SECOM Trust Sy	
SEVRF1	SEVRF1	02.05.2021	<нет>	
SSL.com Root Certi	SSL.com Root Certific	12.02.2041	SSL.com Root C	
Starfield Class 2 Ce	Starfield Class 2 Certi	29.06.2034	Starfield Class 2	$\checkmark$

6. Проверка наличия Сертификата в хранилище сертификатов безопасности закончена.