МОСКОВСКИЙ КРЕДИТНЫЙ БАНК
(публичное акционерное общество)

Руководство по формированию клиентом ключей ЭП и использованию Личного кабинета сертификации

Оглавление

1. Введение

Личный кабинет сертификации (далее – Личный кабинет) представляет собой web-страницу на сайте ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (далее – Банк), защищенную технологией парольной защиты, с использованием которой осуществляется:

– формирование ключа электронной подписи (ключа ЭП) и ключа проверки электронной подписи (ключа проверки ЭП);

– направление в Банк документа «Запрос на изготовление сертификата»;

– получение от Банка сертификата, удостоверяющего ключ ЭП;

– направление в Банк документа «Подтверждение о получении сертификата»,

а также получение от Банка иной информации, необходимой для использования системы дистанционного банковского обслуживания «Ваш Банк Онлайн» и/или сервисов электронного документооборота, предоставляемых Банком Клиентам на основании соответствующих договоров (соглашений) (далее – Система).

Банк предоставляет доступ к Личному кабинету уполномоченному лицу Клиента (далее – Уполномоченное лицо) согласно заявке Клиента на предоставление сертификата и доступа к Системе (далее – Заявка).

Банк направляет на контрактные данные Уполномоченного лица (номер мобильного телефона, адрес электронной почты), указанные в Заявке Клиента, логин и инициализационный пароль для доступа к Личному кабинету, а также sms-коды для подписания документов от имени Клиента и подтверждения иных действий в рамках использования Личного кабинета. Инициализационный пароль подлежит обязательной процедуре его смены.

Банк при регистрации Уполномоченного лица в Системе формирует согласно Заявке Клиента криптографический профиль (далее – криптопрофиль) сертификата, выдача которого осуществляется посредством Личного Кабинета.

Под криптопрофилем понимается совокупность данных, определяющих параметры прав по использованию в Системе ключа ЭП, удостоверенного сертификатом, в соответствии с правами, которыми Клиент наделил Уполномоченное лицо в документе, предоставленном Банку.

Ключ ЭП и удостоверяющий его сертификат могут соответствовать одному из следующих криптопрофилей:

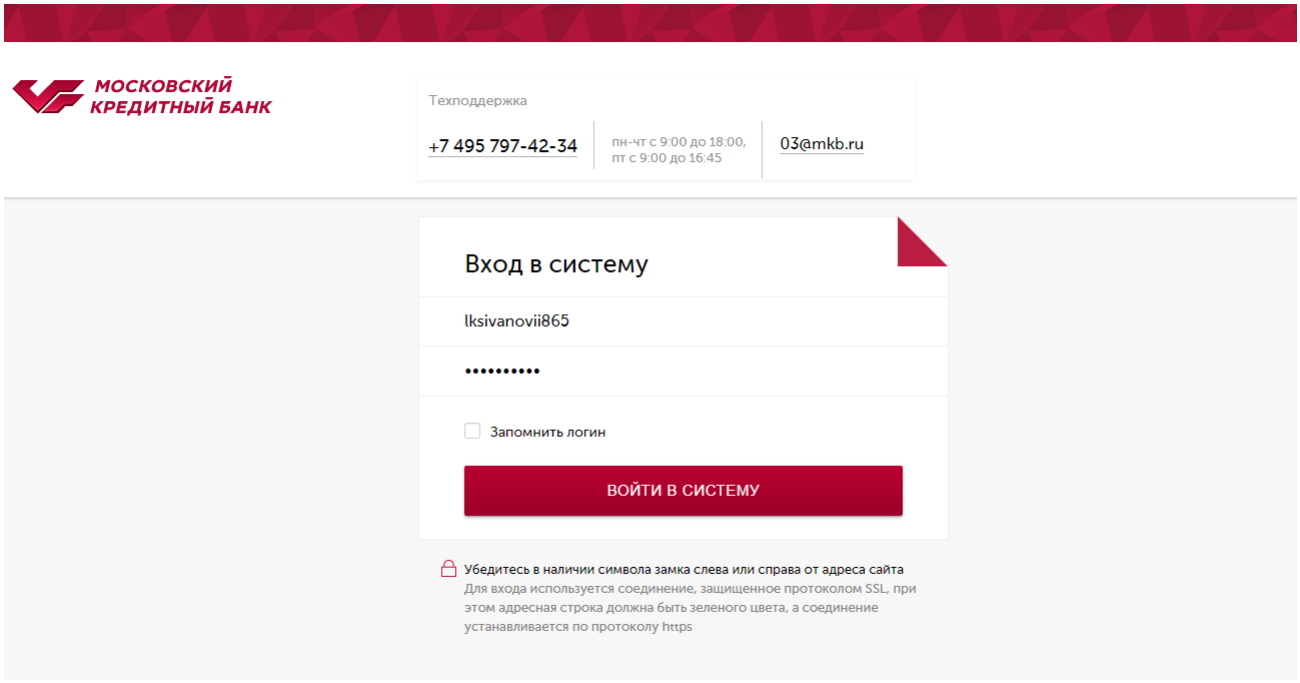
Наименование криптопрофиля	Права
Основной – подпись	Право подписи, а также право совершать сделки с Банком, в том числе заключать договоры

	банковского счета / дистанционного банковского обслуживания / депозита, подписывать дополнения и изменения к Договору и иным договорам, заявки, заявления, акты и иные документы, предусмотренные указанными договорами, кроме ЗАЯВОК-ДОВЕРЕННОСТЕЙ *и/или* право распоряжаться денежными средствами, находящимися на счетах Клиента *и (в случае наделения таким правом)* Разграничение прав доступа к Системе (администрирование)
Основной – просмотр	Разграничение прав доступа к Системе (администрирование) *и/или* Доступ без права подписи

Настоящее Руководство содержит информацию о порядке действий Уполномоченного лица в Личном кабинете по формированию ключа ЭП, ключа проверки ЭП и получения от Банка сертификата, удостоверяющего ключ ЭП, необходимых для работы Уполномоченного лица в Системе.

2. Вход в Личный кабинет

При первом входе перейдите по ссылке, содержащейся в сообщении, отправленном Банком на адрес электронной почты Уполномоченного лица. На стартовой странице Личного кабинета введите инициализационный пароль и нажмите **Войти в систему**:

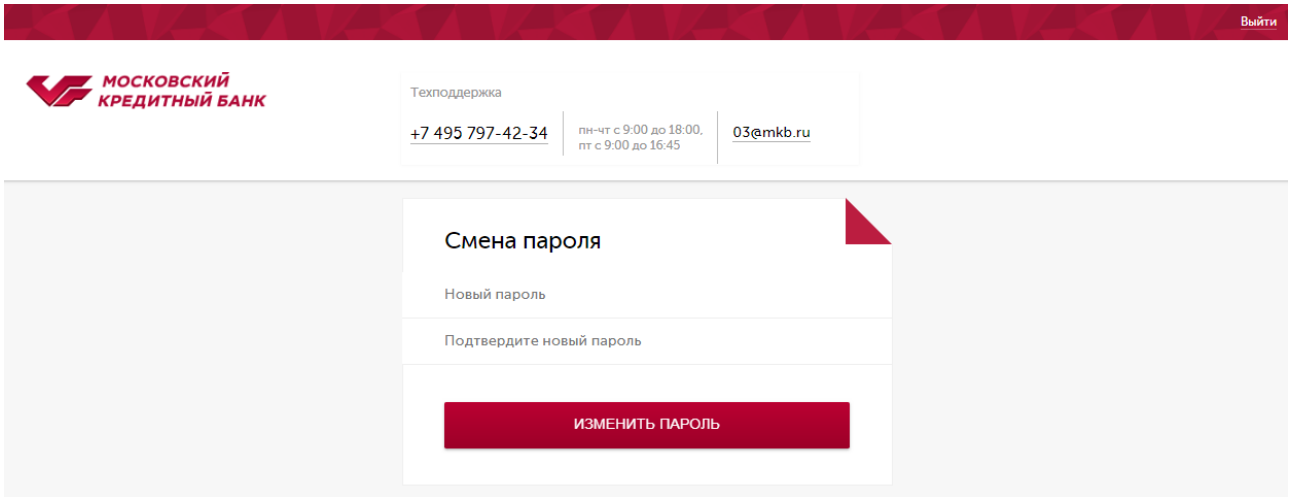


***Логин**, направленный Банком в сообщении на адрес электронной почты Уполномоченного лица, будет заполнен на стартовой странице Личного кабинета автоматически.*

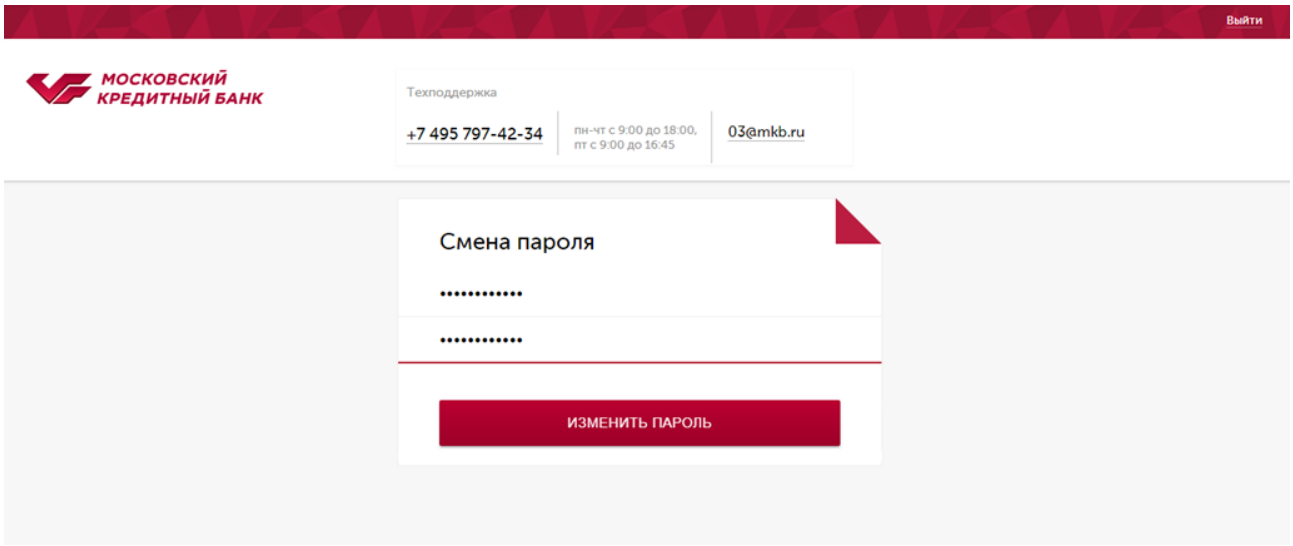
Откроется окно **Смены пароля**, в котором введите новый пароль.
При этом**:**

- длина пароля должна быть не менее 8 символов и он должен содержать:

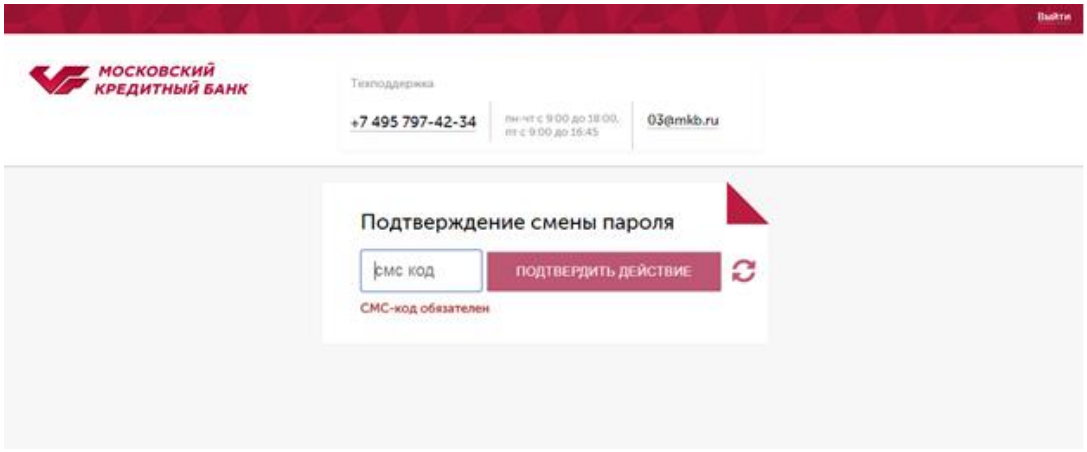
- заглавные буквы
- строчные буквы
- цифры



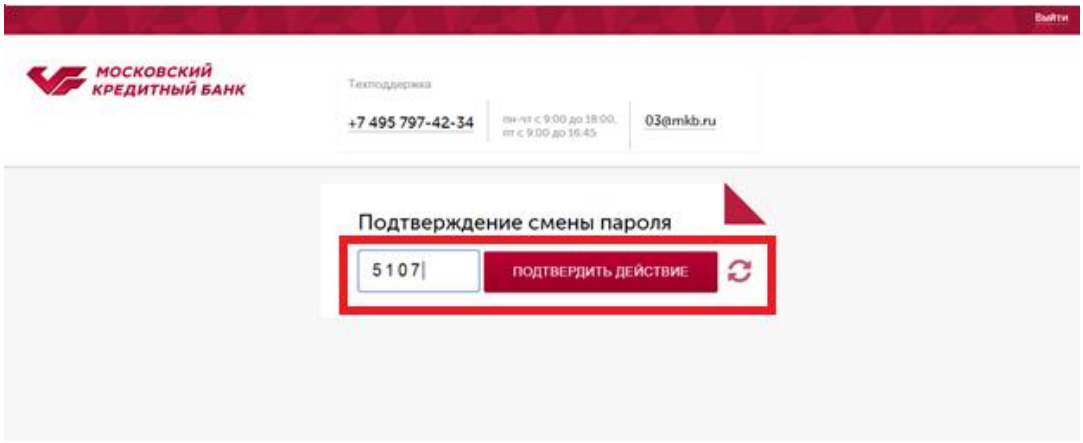
После ввода нового пароля нажмите **Изменить пароль**:



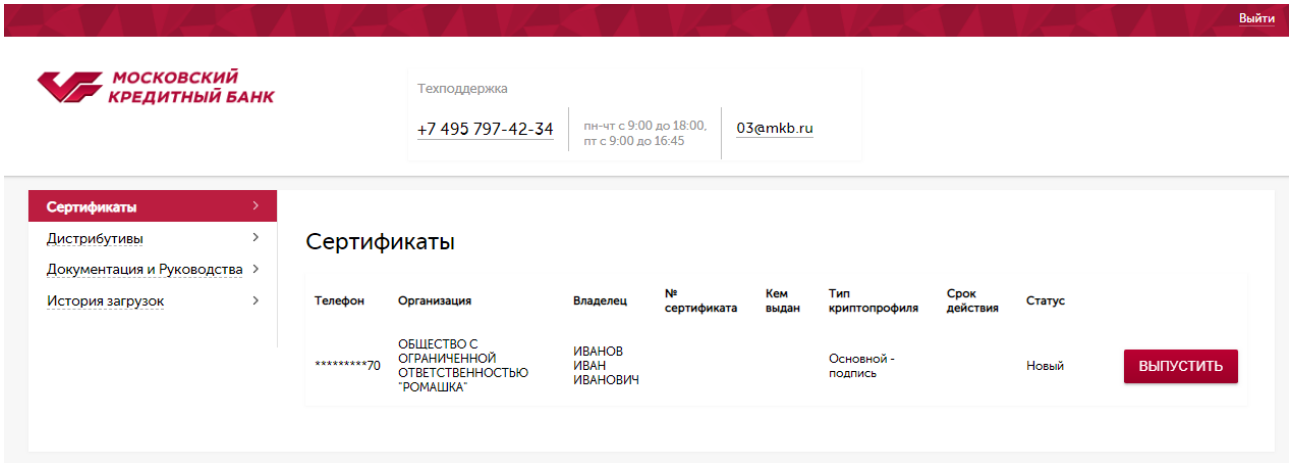
Откроется окно **Подтверждение смены пароля:**



Введите полученный sms-код и нажмите **Подтвердить действие**:



Если sms-код введен верно, вход в Личный кабинет будет выполнен. Откроется главная страница Личного кабинета:



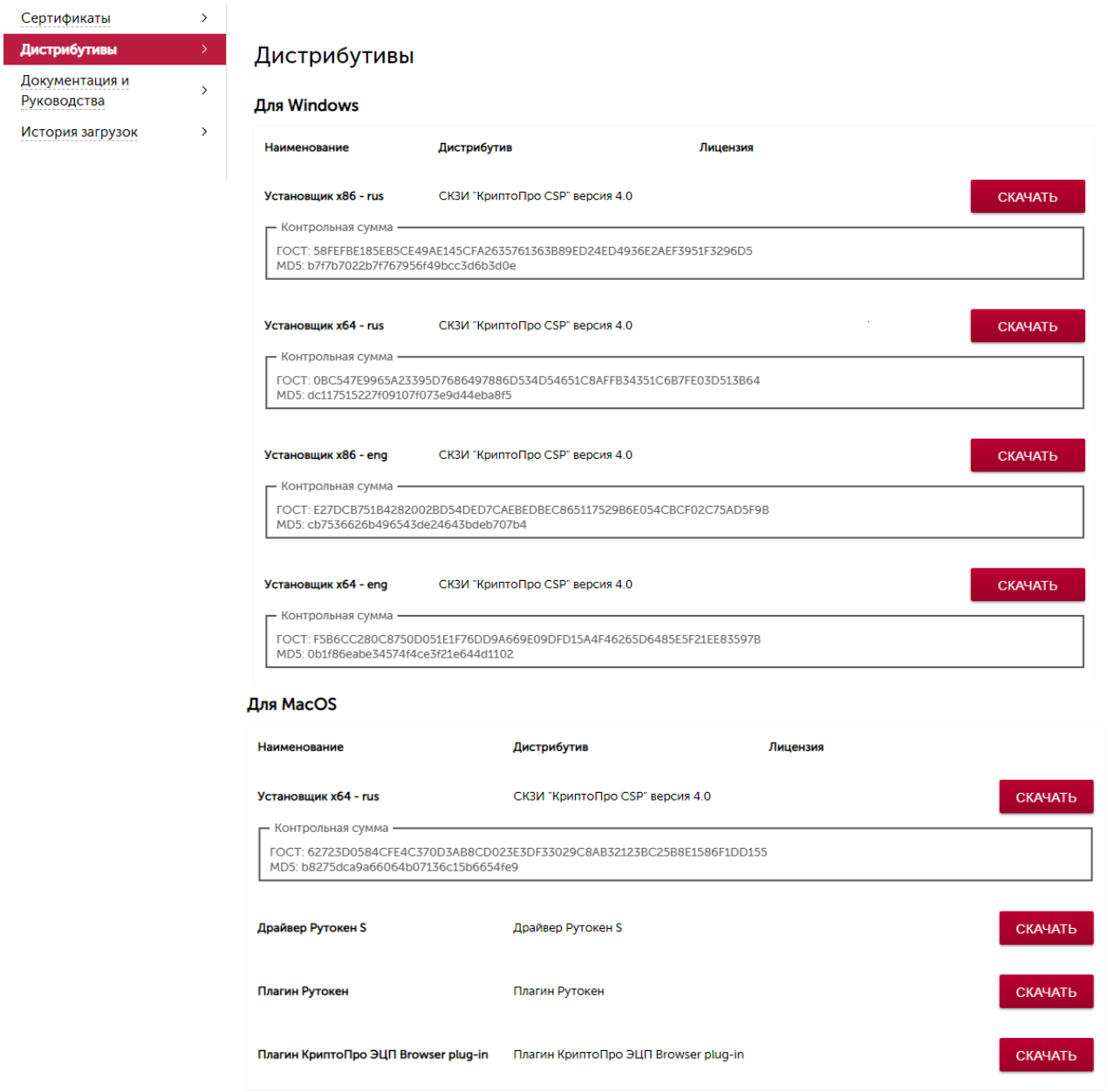
Для последующих входов в Личный кабинет используете установленный пароль.

Если sms-код введен неверно, Банк повторно отправит sms-код для подтверждения пароля. После 3-х неуспешных попыток подтверждения смены пароля данное действие будет временно заблокировано (до 15 минут). По истечении 15 минут Банк повторно отправит sms-код для подтверждения пароля.

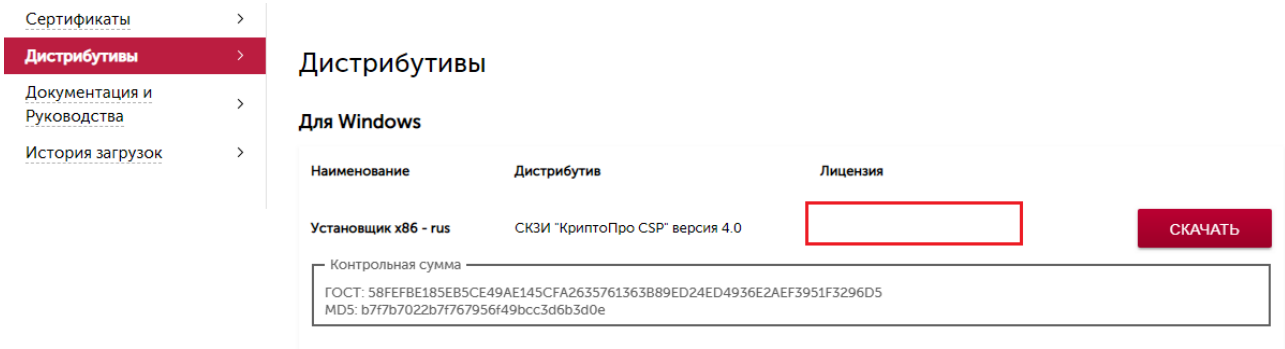
> *В случае утраты Уполномоченным лицом пароля в процессе эксплуатации Личного кабинета (пароль забыт) необходимо обратиться в службу технической поддержки систем дистанционного банковского обслуживания посредством Контакт-центра Банка. При обращении необходимо использовать кодовое слово данного Уполномоченного лица, указанного в Заявке Клиента.*

3. Установка программного обеспечения

Для формирования ключа ЭП, ключа проверки ЭП и создания ЭП при работе в Системе необходимо скачать и установить программное обеспечение (ПО) СКЗИ «КриптоПро CSP» версии 4.0, плагина Cadescom, драйвер Рутокена S/ЭЦП 2.0. Для этого перейдите в раздел **Дистрибутивы.**
Напротив установщика необходимого комплекта дистрибутивов нажмите **Скачать:**



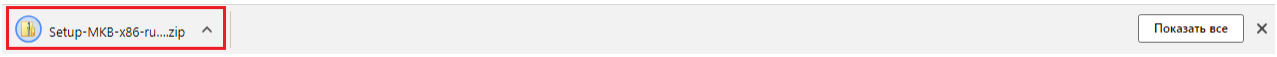
*После скачивания комплекта дистрибутивов в разделе **Дистрибутивы** в поле **Лицензия** отобразится серийный номер лицензии на право использования СКЗИ «КриптоПро CSP» версии 4.0, являющийся также ключом установки данного ПО:*



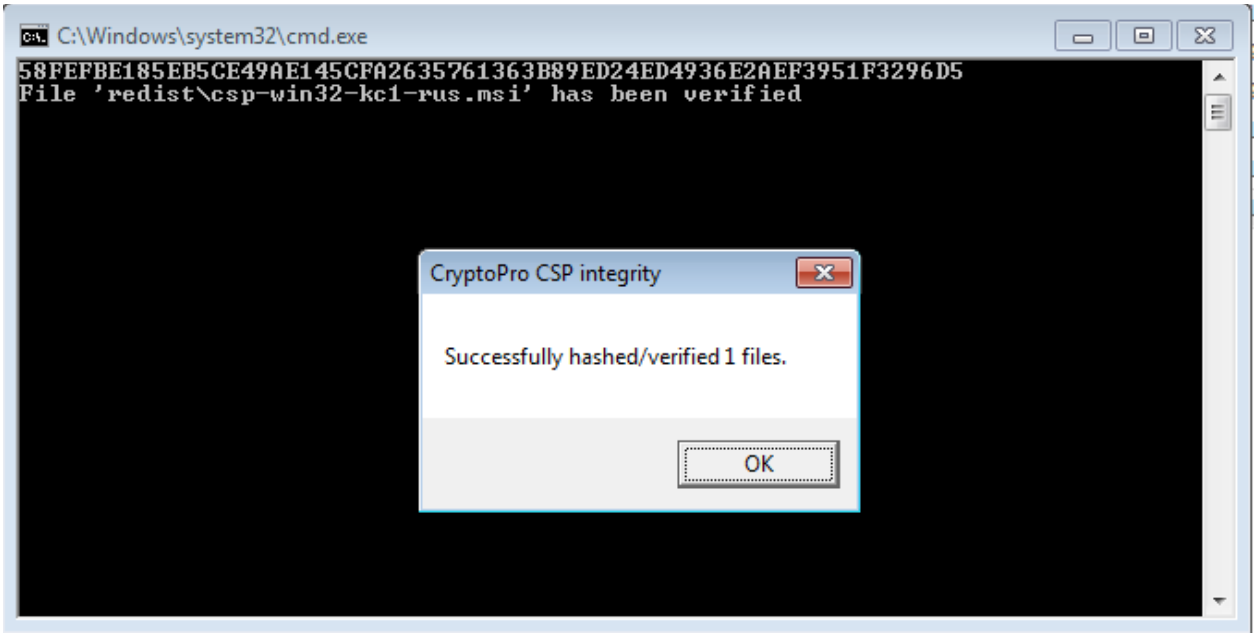
Вместе с дистрибутивами на странице загрузки размещаются контрольные суммы установочных модулей и документации СКЗИ. Контрольные суммы рассчитываются в соответствии с ГОСТ Р 34.11 94 с учётом RFC 4357, а также md5:

ВНИМАНИЕ! Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации.

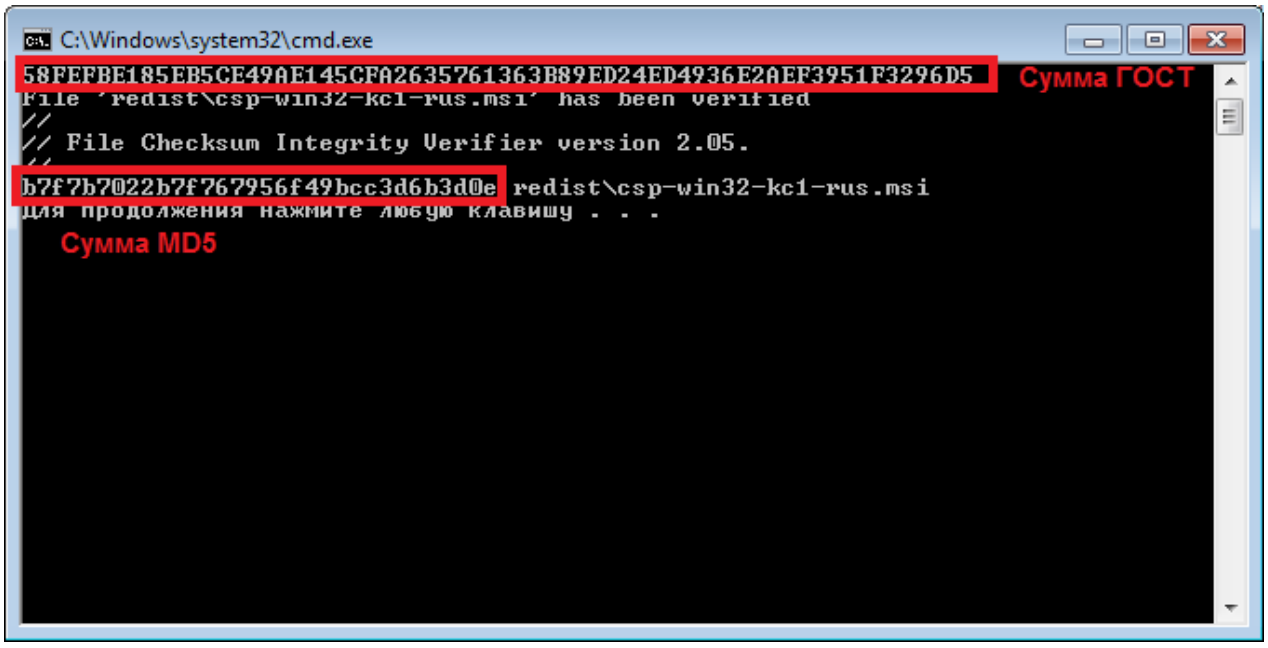
Для проверки контрольных сумм закаченных дистрибутивов СКЗИ необходимо разархивировать скачанный архив дистрибутивов и запустить файл **Контрольная сумма ГОСТ и md5** ***csp-win32-kc1-rus.msi*.bat** (в зависимости от версии Установщика):



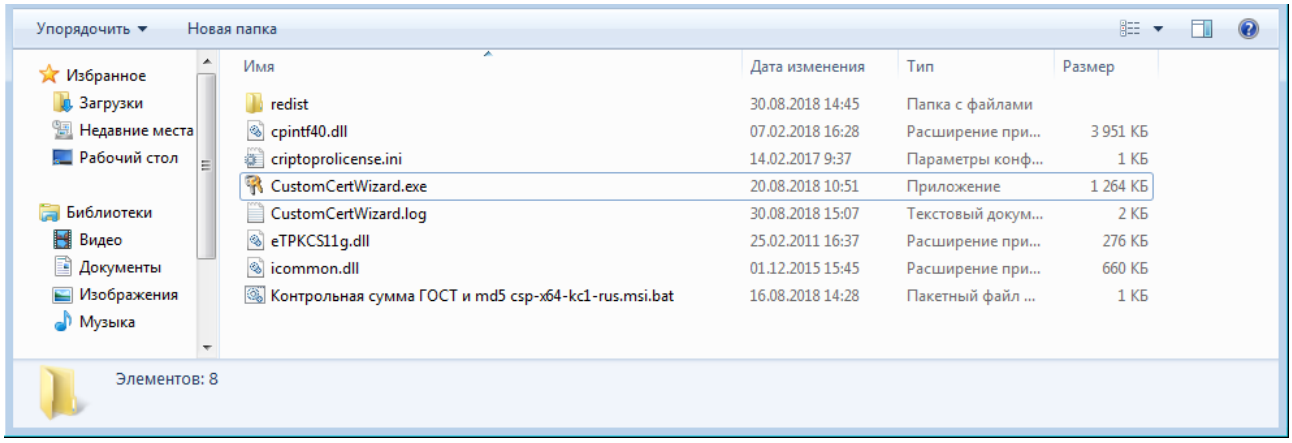
Откроется окно, в котором будет выведено сообщение о проведенной сверке контрольных сумм, заложенных в дистрибутив, с передаваемой суммой. Если контрольные суммы ГОСТ совпали, отобразится окно с надписью **Successfully hashed/verified 1 files**. Необходимо нажать ОК:



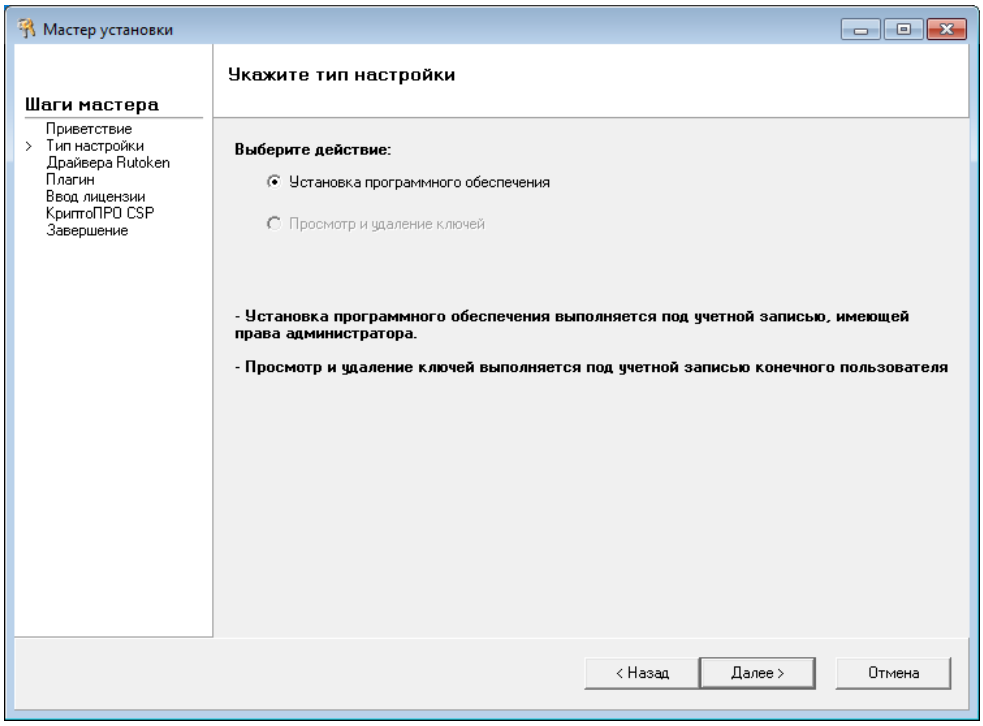
Далее в окне отобразится md5 сумма. Произведите сверку контрольных сумм и закройте окно:



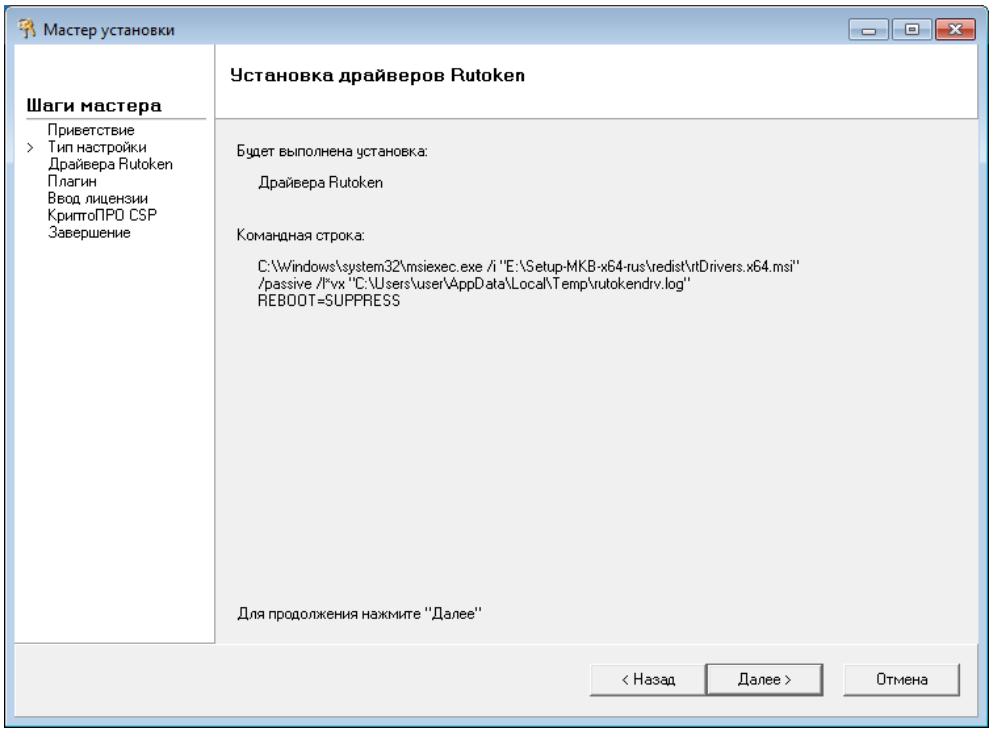
Для установки необходимого ПО запустите приложение CustomCertWizard.exe:



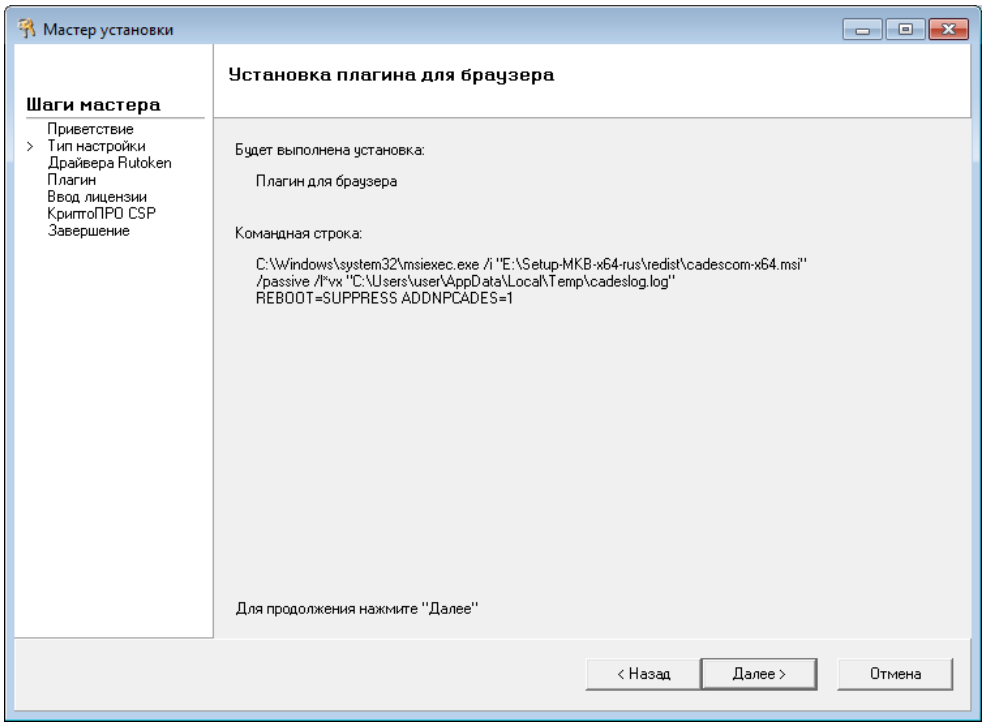
В открывшемся окне нажмите **Далее:**



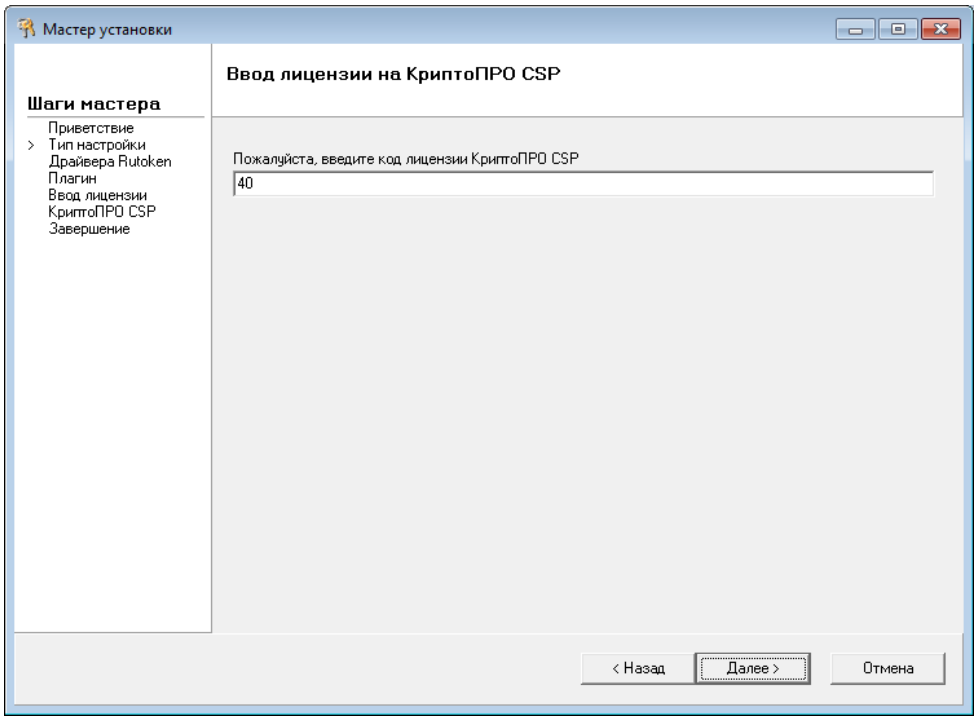
Для установки драйверов Rutoken S/ЭЦП 2.0 в открывшемся окне нажмите **Далее:**



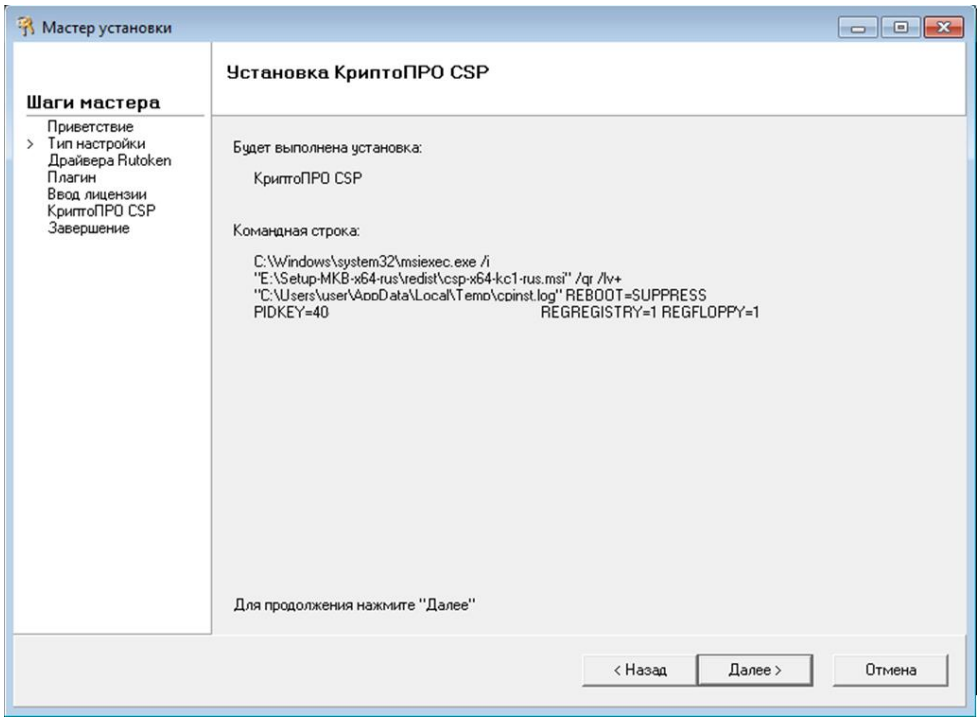
Для установки плагина для браузера в открывшемся окне нажмите **Далее:**



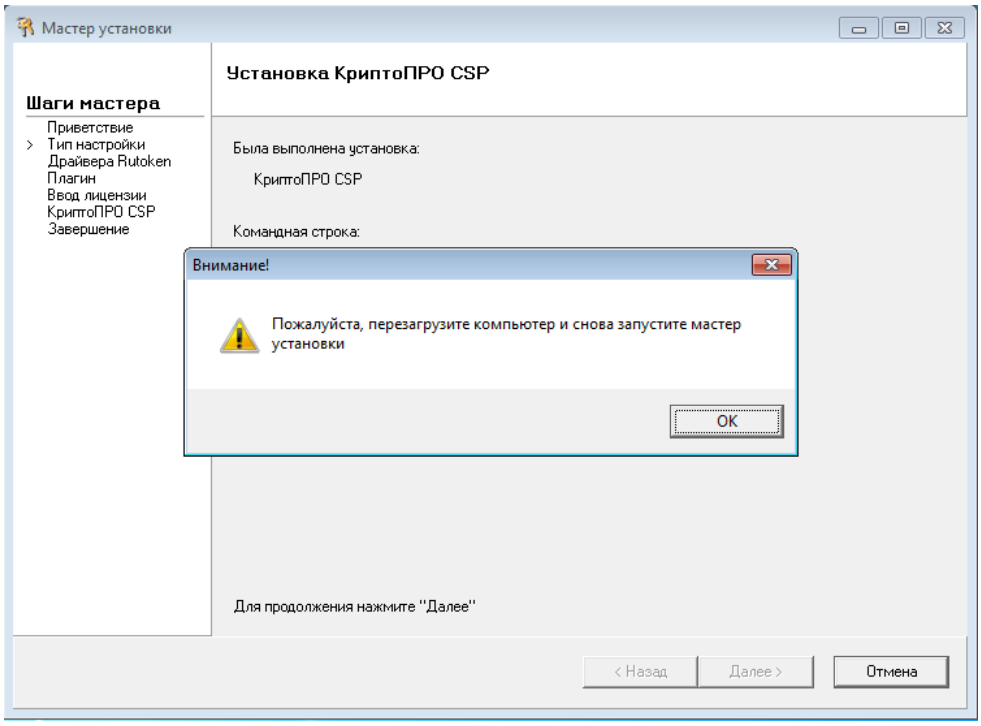
Номер лицензии на право использования СКЗИ «КриптоПро CSP» подтянется автоматически. Нажмите **Далее:**



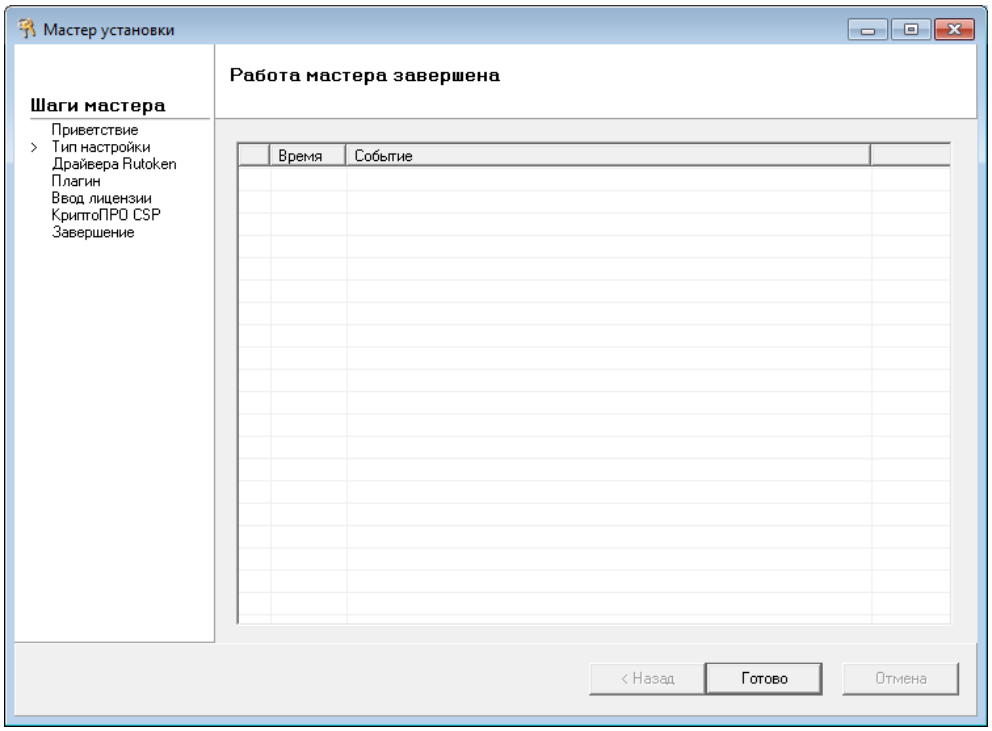
В открывшемся окне нажмите **Далее:**



В открывшемся окне нажмите **ОК**

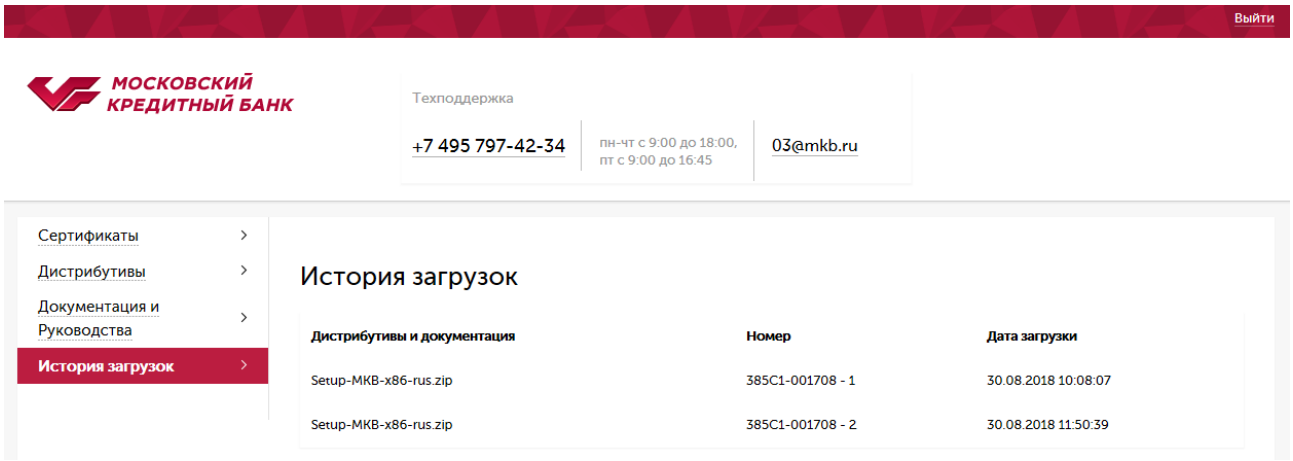


В открывшемся окне нажмите **Готово.**



Необходимый комплект дистрибутивов установлен. Перезагрузите компьютер.

Для просмотра истории скачиваний и серийного номера скачанного дистрибутива СКЗИ «КриптоПро CSP» перейдите в раздел **История загрузок**:



4. Формирование ключа ЭП, ключа проверки ЭП и получение сертификата

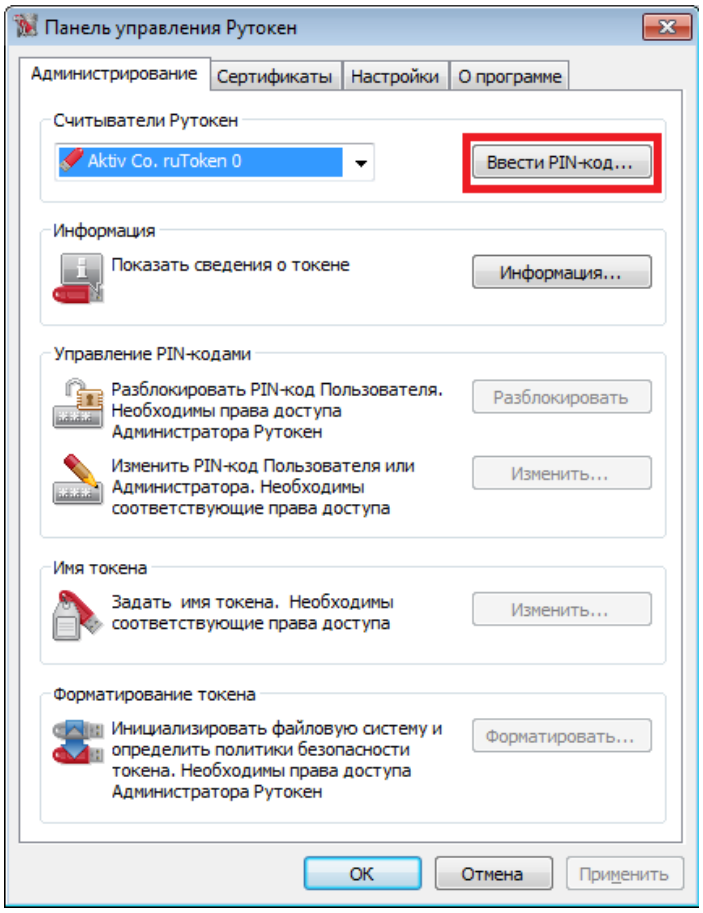
ВНИМАНИЕ! *Пропустите нижеследующий блок «Форматирование Рутокен S/ЭЦП 2.0», если вы используете Рутокен S/ЭЦП 2.0, на котором хранятся действующие ключи ЭП, используемые в Системе.*

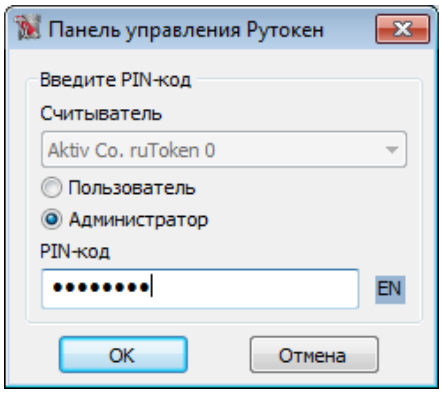
ВАЖНО! *При форматировании ключевого носителя Рутокен S/ЭЦП 2.0, ранее сохраненная информация будет уничтожена!*

Форматирование Рутокен S/ЭЦП 2.0:

Если вы сохраняете ключи ЭП на **новый** Рутокен S/ЭЦП 2.0 (USB-токен) необходимо предварительно сменить его стандартные пароли на пин-код (PIN-код), известный только Уполномоченному лицу.

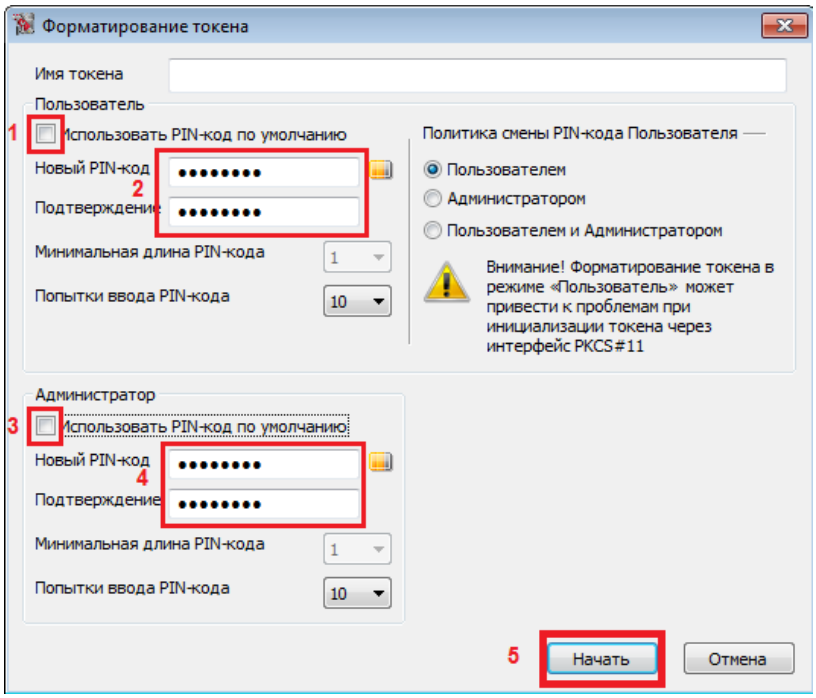
Запустите **Панель управления Рутокен** (ПУСК – Все программы – Rutoken – Панель управления Рутокен).
В списке **Считыватели Рутокен** необходимо выбрать необходимый Рутокен и авторизоваться (ввести pin-код) с паролем администратора (по умолчанию):





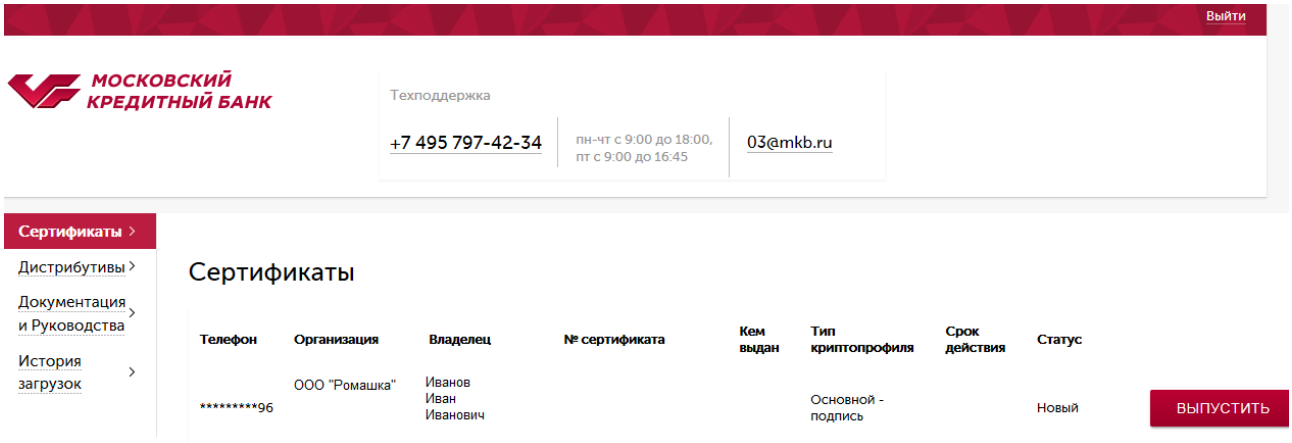
Пароль администратора на Рутокен (по умолчанию) – 87654321
Пароль пользователя на Рутокен (по умолчанию) – 12345678

Необходимо нажать кнопку «**Форматировать**» и в открывшейся форме установить необходимые PIN-коды пользователя (необходим для работы в Системе) и администратора. Для этого в соответствующем разделе необходимо снять галку, ввести пароль и его подтверждение и нажать кнопку **Начать:**

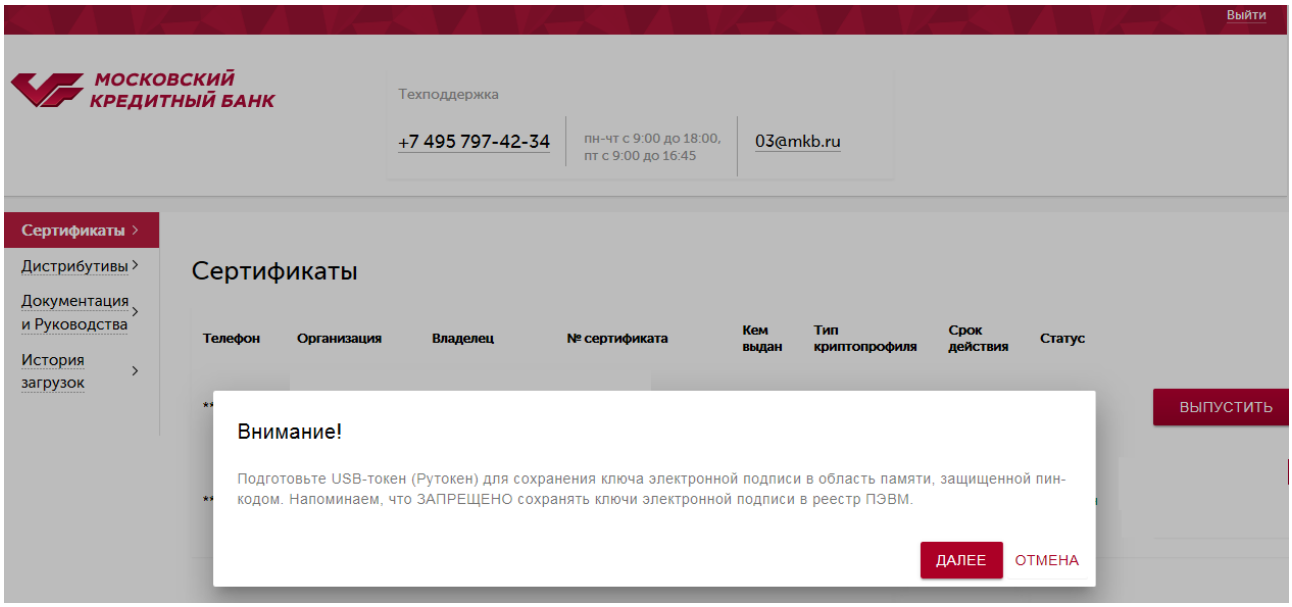


Формирование ключей:

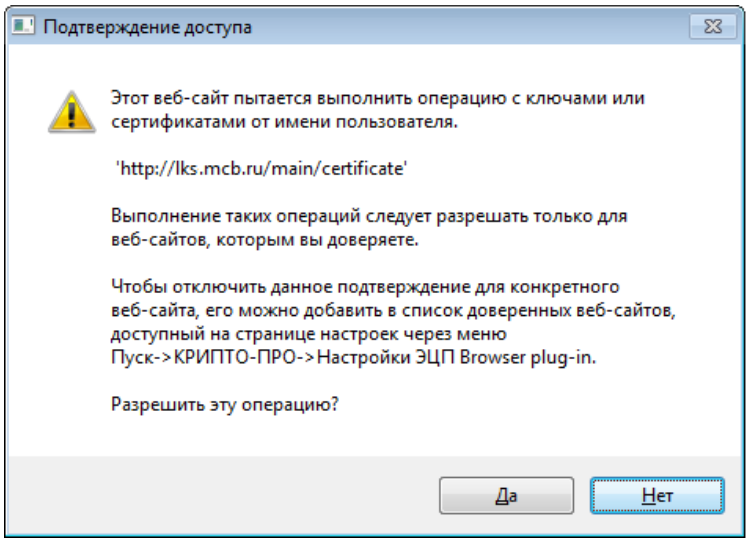
Для формирования ключей перейдите в раздел **Сертификаты**. В списке доступных криптопрофилей нажмите **Выпустить** напротив криптопрофиля со статусом **Новый**:



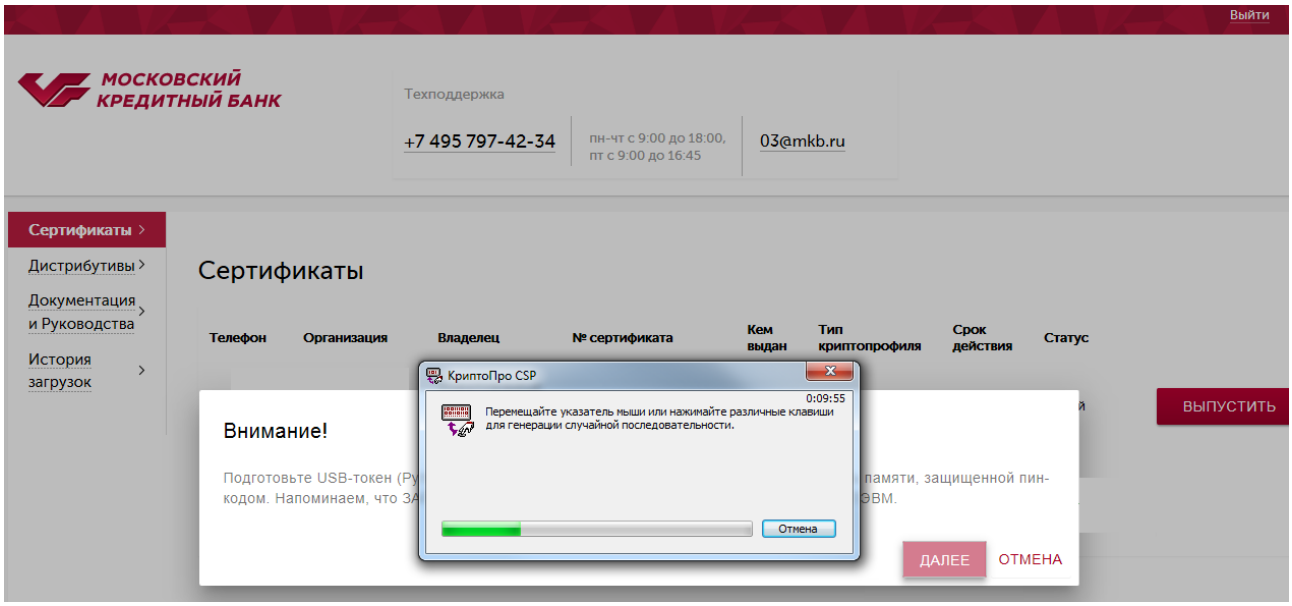
Подключите Рутокен S/ЭЦП 2.0 к компьютеру и нажмите **Далее**:



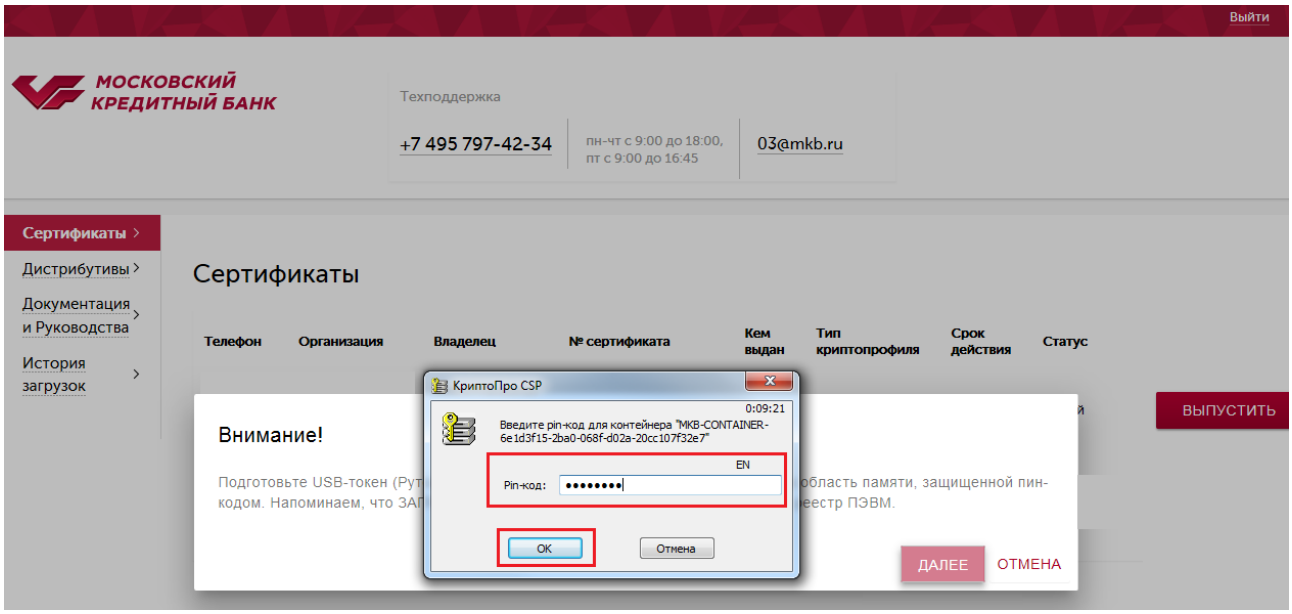
В открывшемся окне нажмите **Да:**



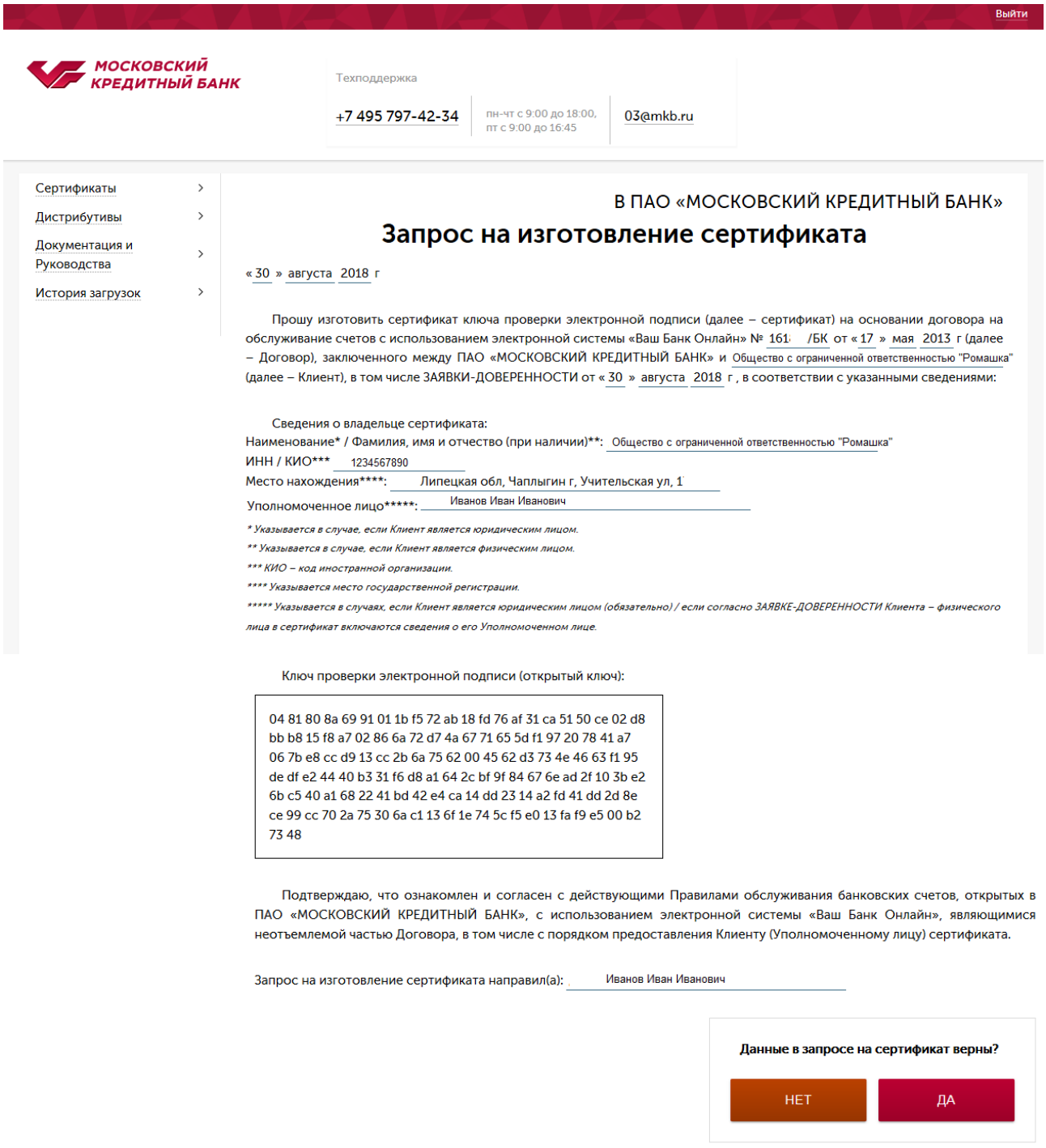
Запустится процесс формирования ключей. В процессе работы датчика случайных чисел необходимо перемещать указатель мыши или нажимать различные клавиши на клавиатуре для генерации случайной последовательности:



После окончания работы датчика случайных чисел откроется окно, в котором введите пин-код для Рутокен S/ЭЦП 2.0 и нажмите **ОК**:

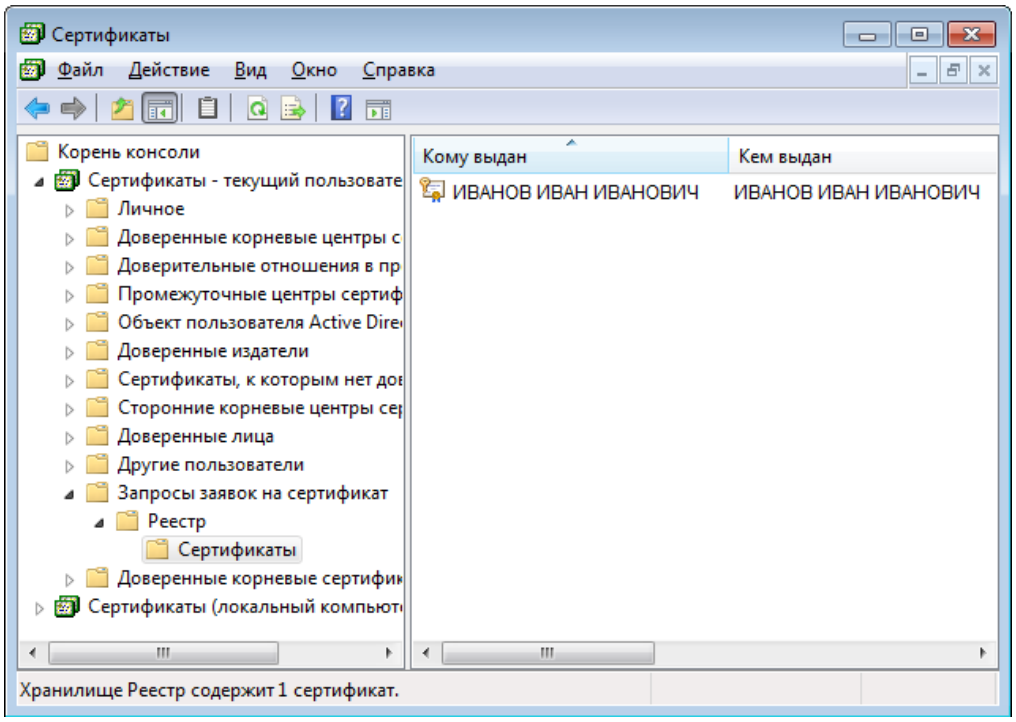


Откроется форма документа «**Запрос на изготовление сертификата**»:

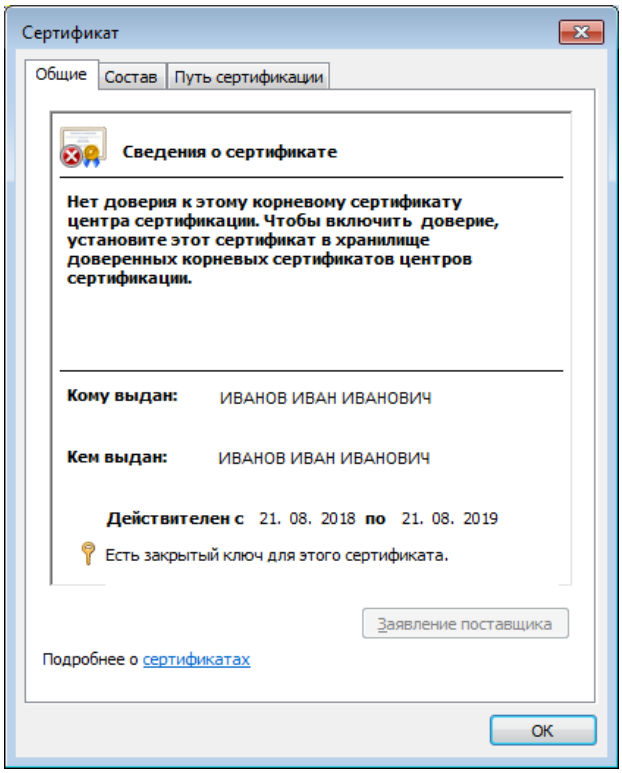


До отправки в Банк «**Запроса на изготовление сертификата**» проверьте сведения, указанные в нем. Для проверки сведений о владельце сертификата и ключе проверки ЭП (открытом ключе) выполните:
Пуск – Все программы – КРИПТО-ПРО – Сертификаты (или при помощи комбинации клавиш **«Win+R»** в открывшемся окне введите команду **certmgr.msc** и нажмите **«Выполнить»**).
Необходимо перейти в папку **Сертификаты-текущий пользователь – Запросы заявок на сертификат – Реестр – Сертификаты**.

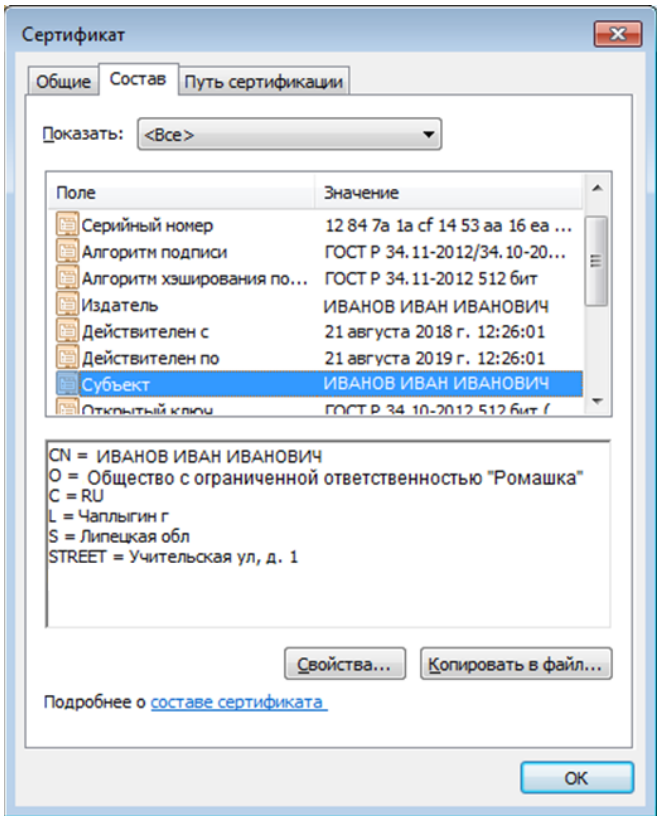
Выберите нужный запрос на сертификат двойным нажатием мыши:



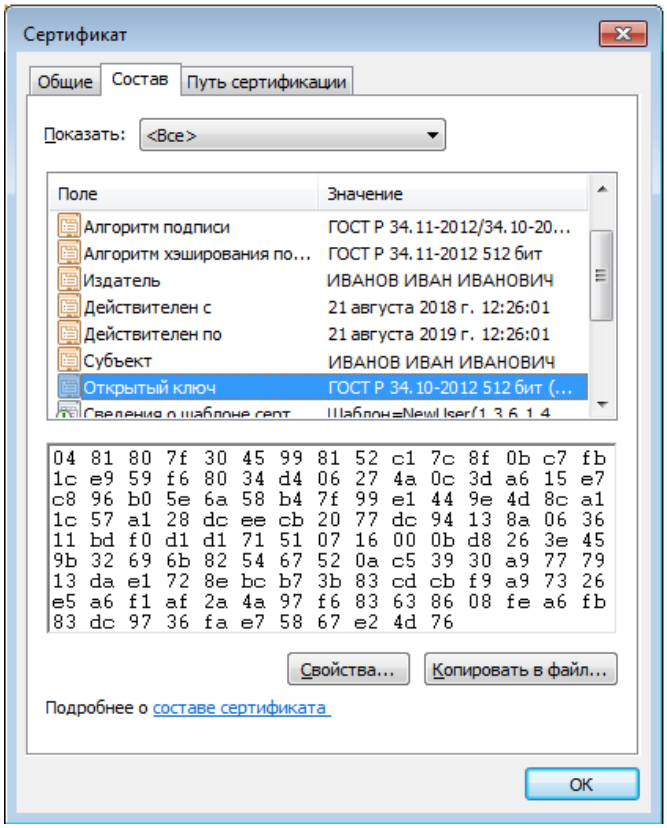
Откроется запрос на сертификат:



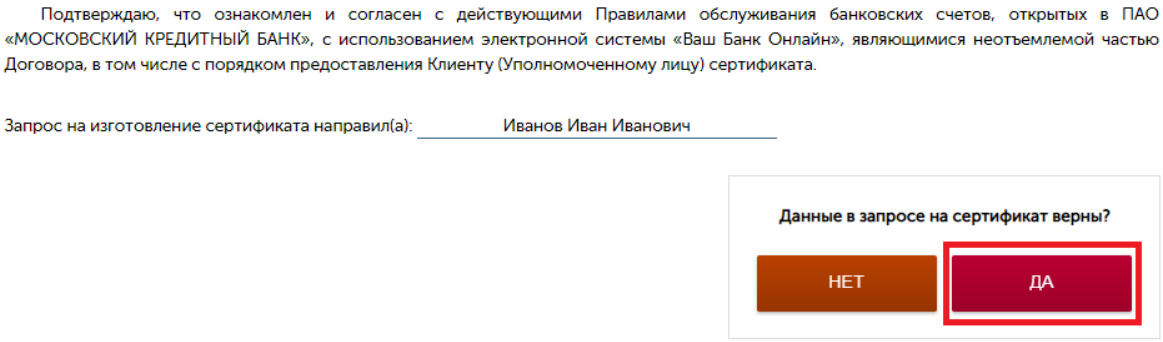
Для проверки наименования Клиента, место нахождения и ФИО Уполномоченного лица перейдите во вкладку **Состав** и выберите раздел **Субъект**:



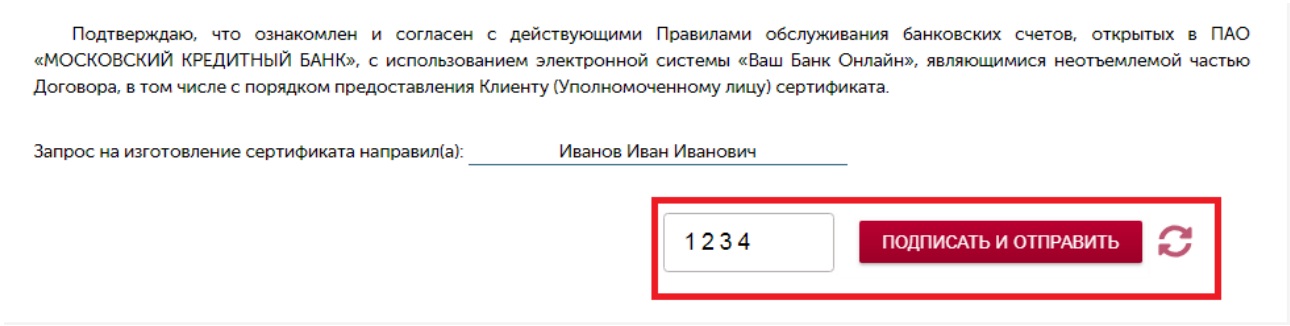
Для проверки ключа проверки ЭП (открытого ключа) во вкладке **Состав** выберите раздел **Открытый ключ:**



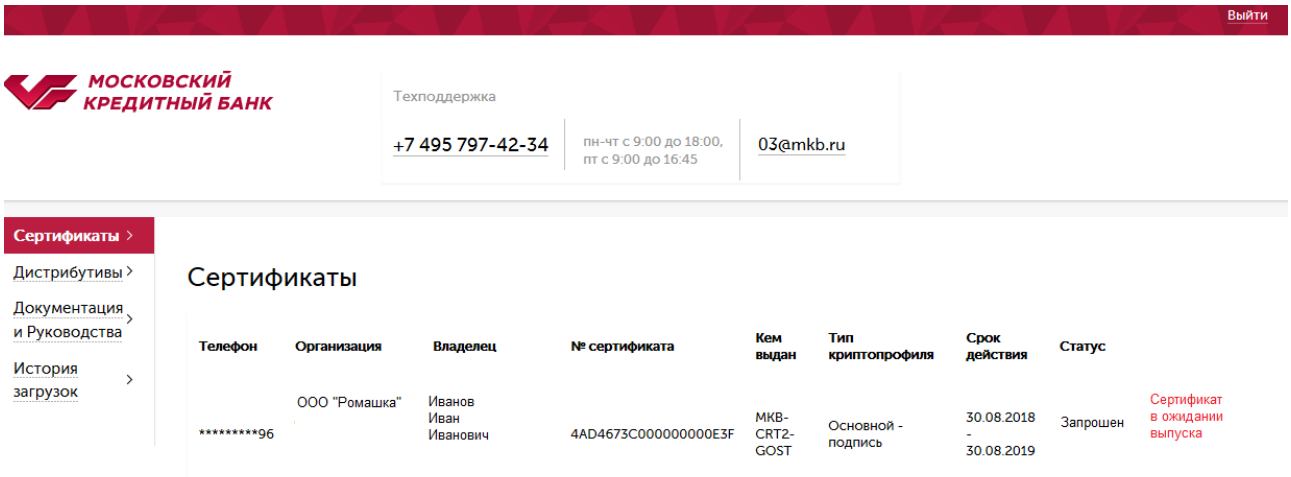
Если данные в «**Запросе на изготовление сертификата**» верны, подтвердите их корректность, нажав в форме документа **Да**:



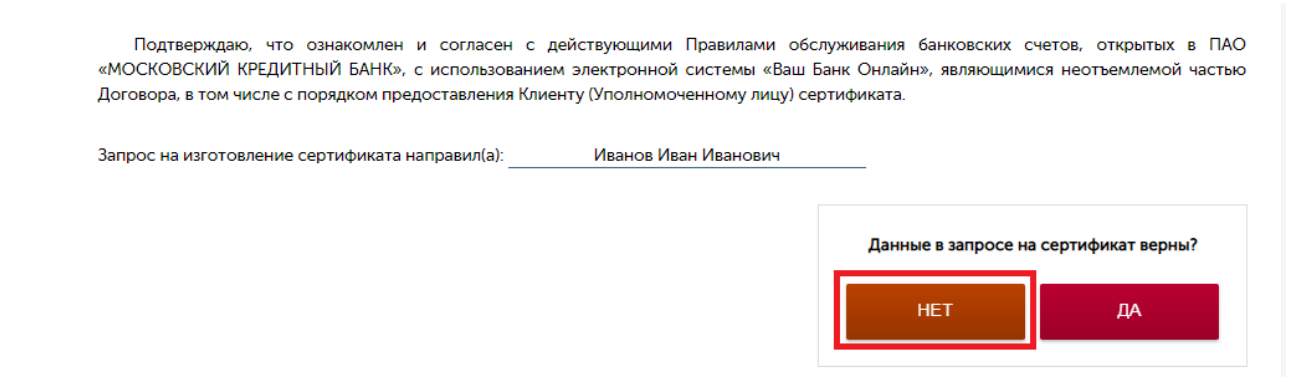
В форме **«Запроса на изготовление сертификата»** отобразится окно для подписания документа sms-кодом и отправки в Банк. Введите полученный sms-код и нажмите **Подписать и отправить**:



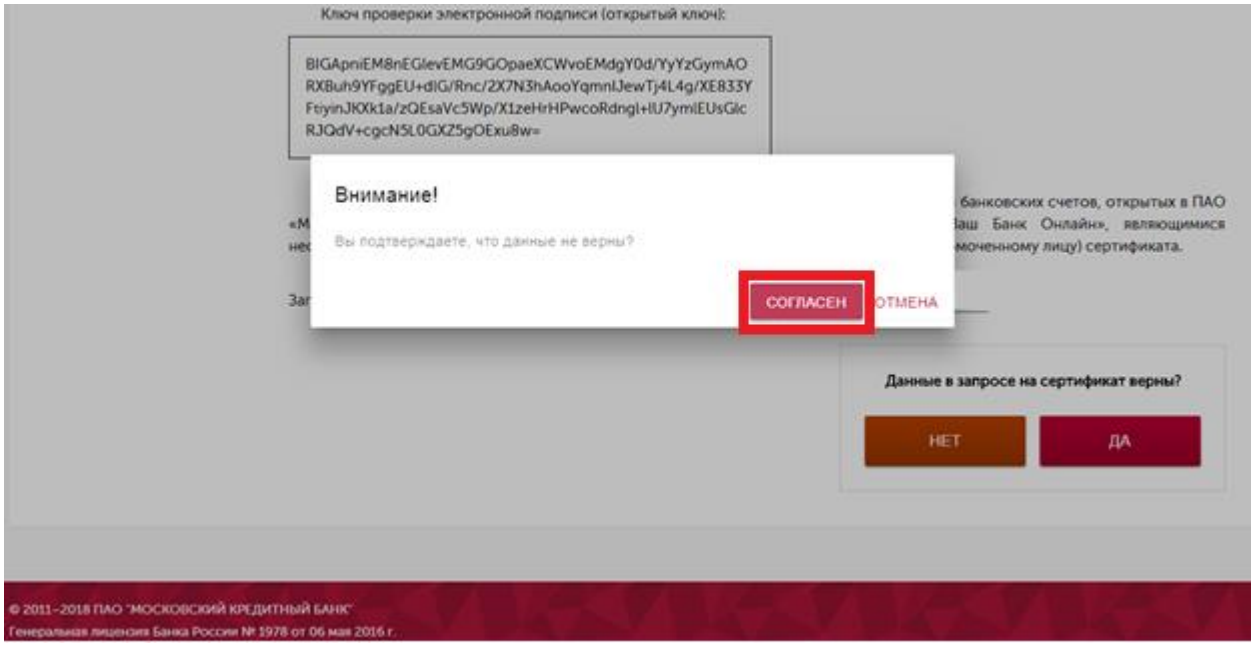
Если sms-код введен верно, документ «Запрос на изготовление сертификата» будет направлен в Банк и статус криптопрофиля изменится на **Сертификат в ожидании выпуска**:



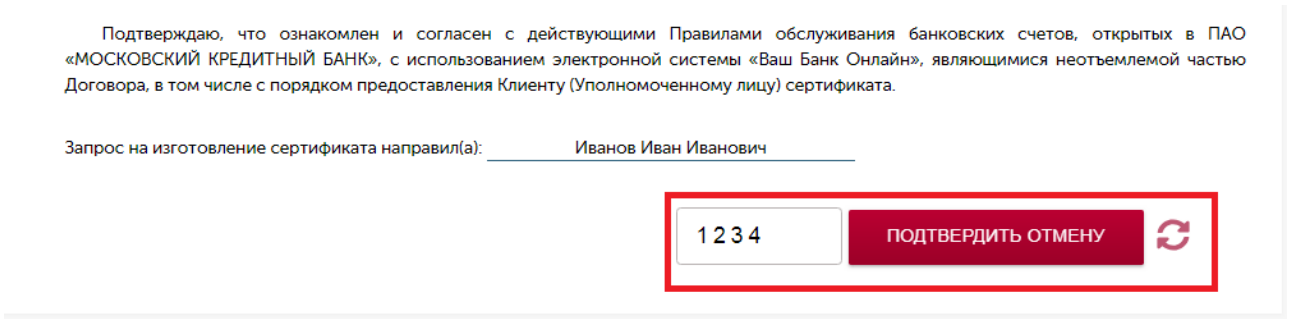
Если данные в «**Запросе на изготовление сертификата**» неверны, нажмите **Нет**:



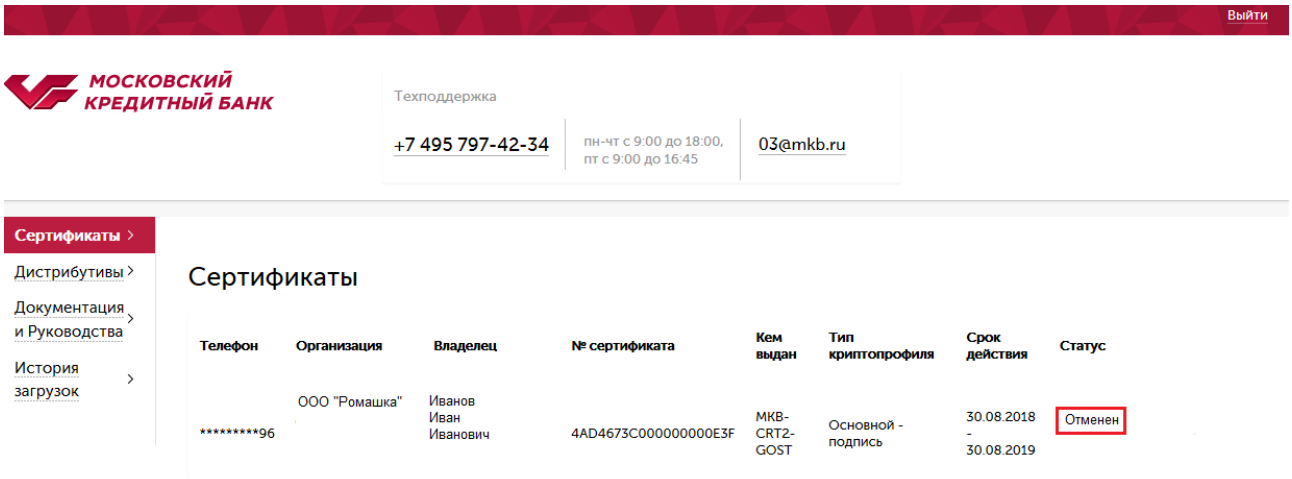
Подтвердите, что данные неверны, нажав **Согласен:**



В форме **«Запроса на изготовление сертификата»** отобразится окно для подтверждения отмены отправки документа в Банк. Введите полученный sms-код и нажмите **Подтвердить отмену**

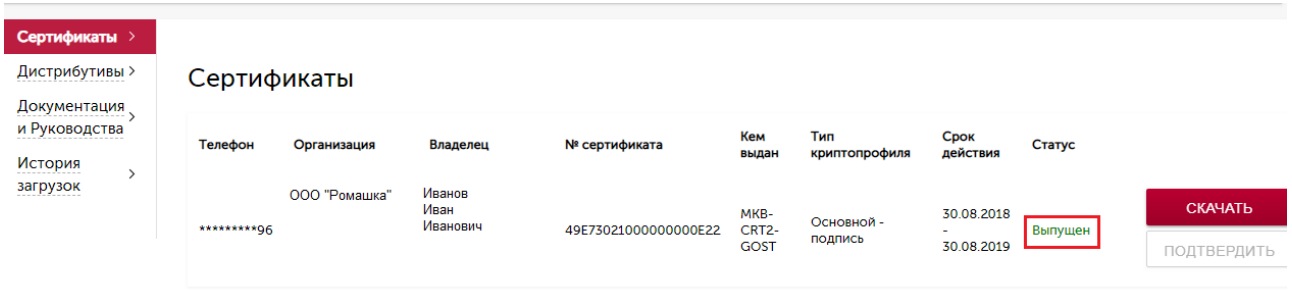


Процедура получения сертификата прекратится и статус криптопрофиля изменится на **Отменен**:

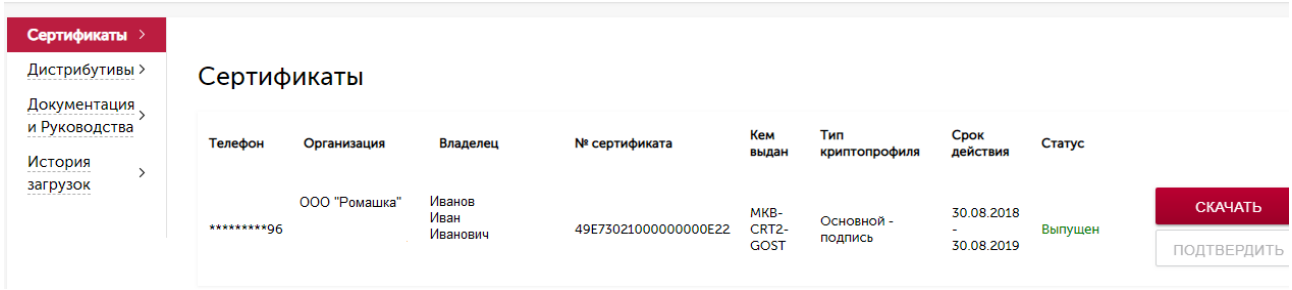


Сведения в документе «Запрос на изготовление сертификата» соответствуют сведениям, указанным Клиентом в Заявке. В случае неверных сведений в документе «Запрос на изготовление сертификата» в отношении владельца сертификата (Клиента и его Уполномоченного лица) Клиенту необходимо обратиться к клиентскому менеджеру / в обслуживающий дополнительный офис Банка и предоставить новую Заявку на данное Уполномоченное лицо, а также документы, подтверждающие изменение указанных ранее сведений. В случае неверных сведений в отношении ключа проверки ЭП Уполномоченному лицу необходимо обратиться в службу поддержки систем ДБО посредством Контакт-центра.

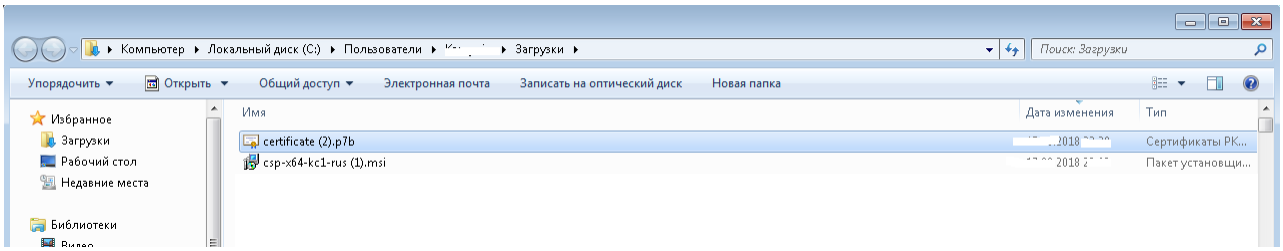
После выпуска Банком сертификата статус криптопрофиля изменится на **Выпущен**:



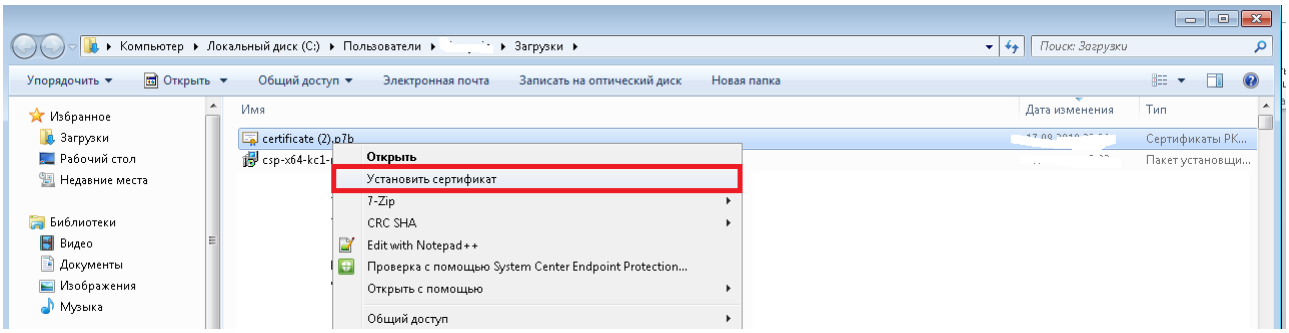
Необходимо скачать и установить сертификат на компьютер. Для скачивания нажмите **Скачать:**



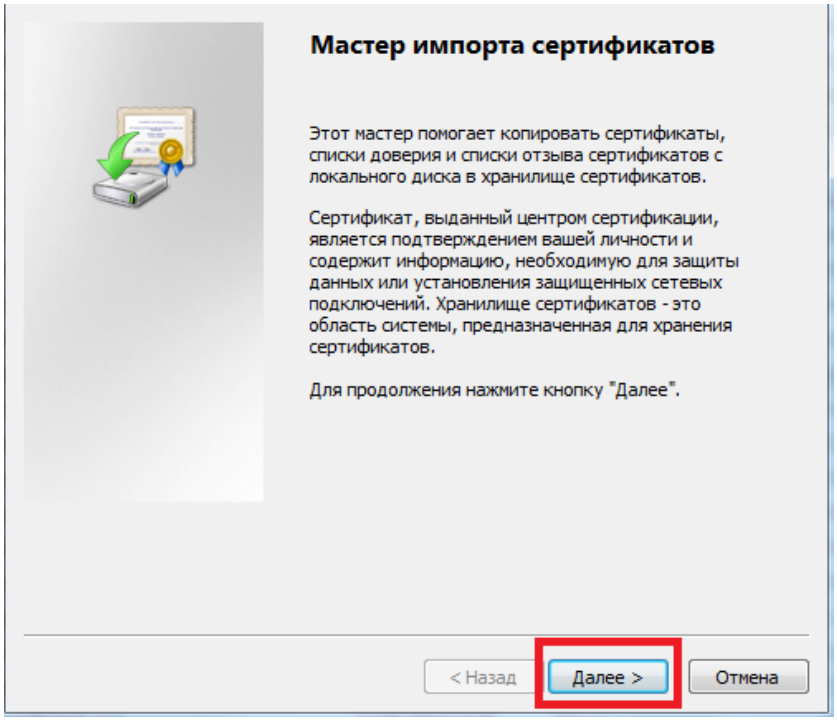
Скачанный сертификат сохраняется в папке **Загрузки**:



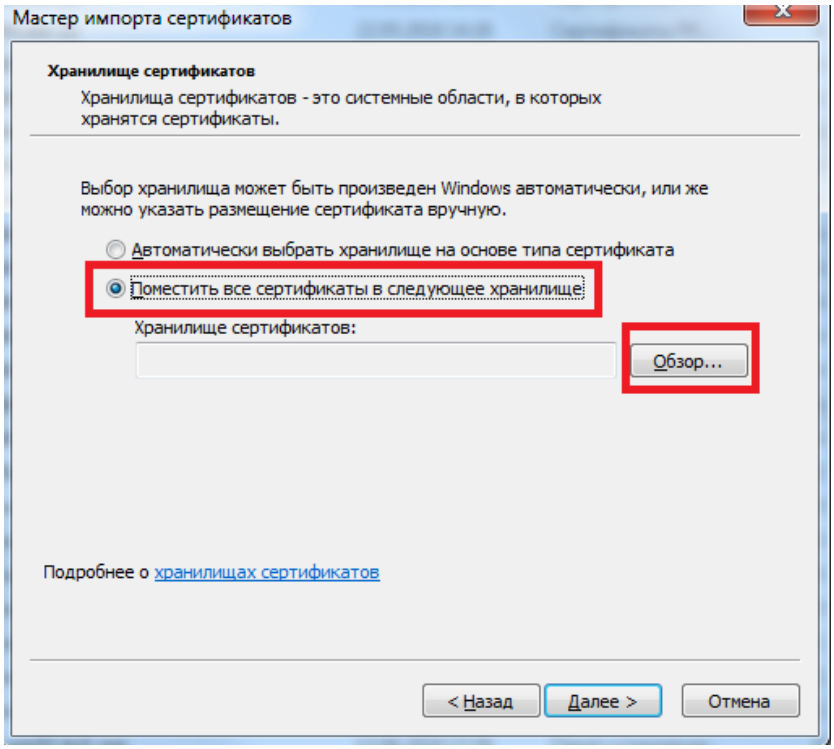
Для установки сертификата нажмите правой кнопкой мыши на сертификат и выберите действие **Меню – Установить сертификат**:



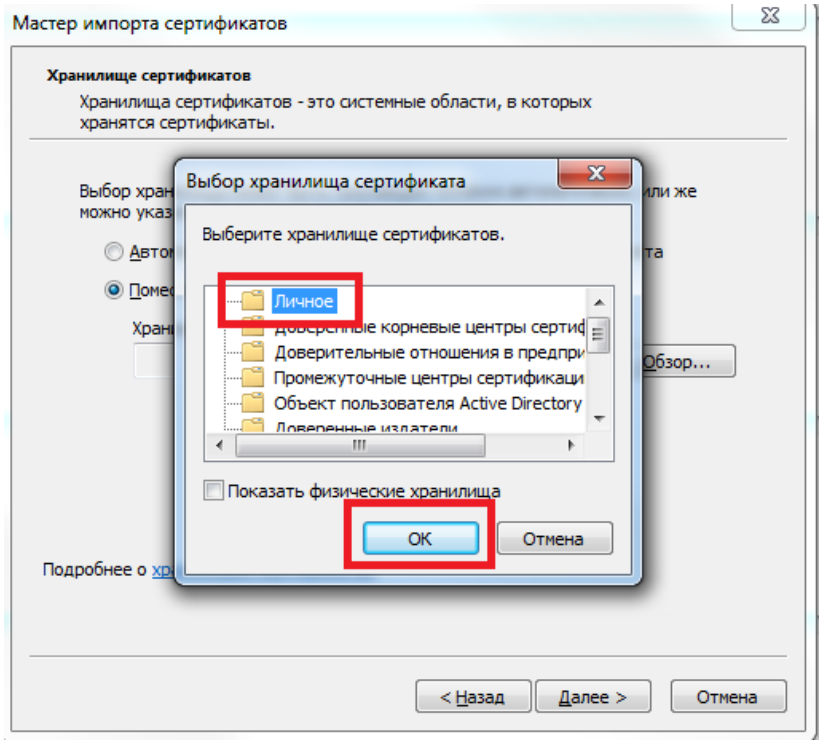
Запустится **Мастер импорта сертификатов**, нажмите **Далее**:



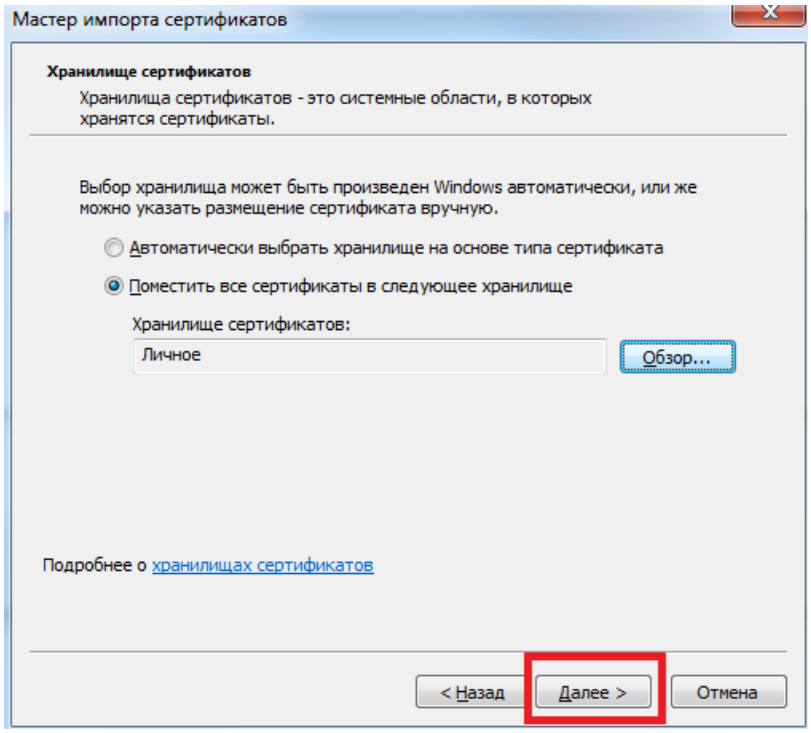
В открывшемся окне выберите **Поместить все сертификаты в следующее хранилище** и нажмите **Обзор**:



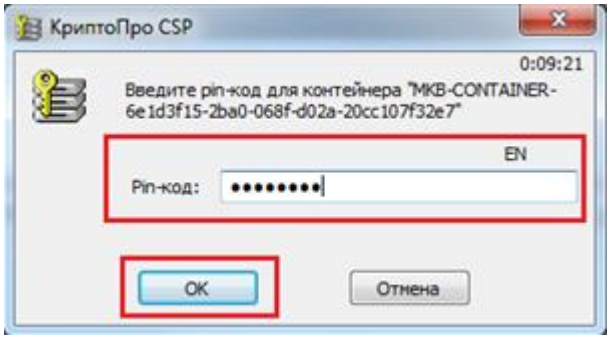
Выберите хранилище **Личное** и нажмите **ОК**:



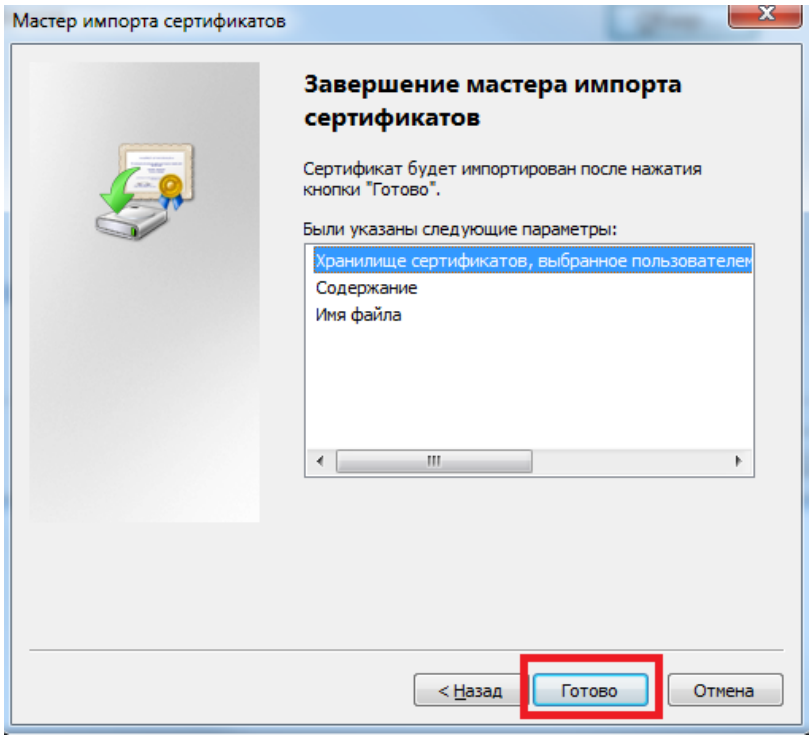
Затем нажмите **Далее**:



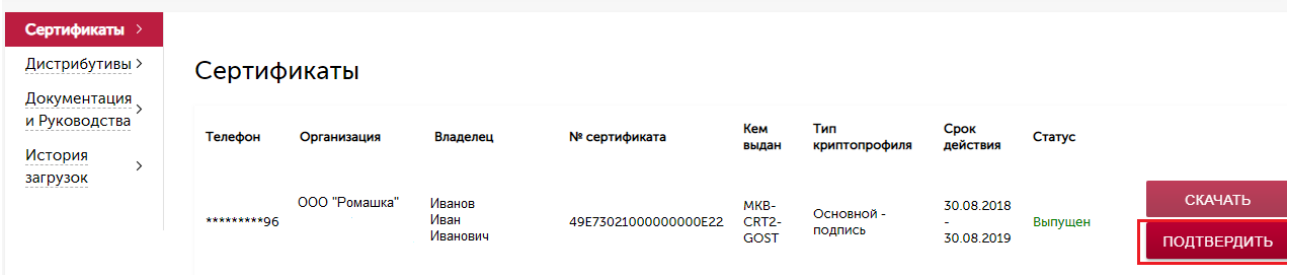
В открывшемся окне введите пин-код для Рутокен S/ЭЦП 2.0 и нажмите **ОК**:



Для завершения установки сертификата нажмите **Готово**:



После установки сертификата необходимо отправить в Банк документ «Подтверждение о получении сертификата». Для этого нажмите кнопку **Подтвердить**:



Откроется форма документа «**Подтверждение о получении сертификата**»:

Выйти

МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

Техподдержка

+7 495 797-42-34 | пн-чт с 9:00 до 18:00, пт с 9:00 до 16:45 | 03@mkb.ru

- Сертификаты
- Дистрибутивы
- Документация и Руководства
- История загрузок

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

Подтверждение о получении сертификата

« 30 » августа 2018 г

Настоящим подтверждаю получение сертификата ключа проверки электронной подписи (далее – сертификат) в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № 161 /БК от « 17 » мая 2013 г (далее – Договор), заключенным между ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (далее – Банк) и Общество с ограниченной ответственностью "Ромашка" (далее – Клиент), при этом:

1. Подтверждаю, что принял от Банка сертификат в форме электронного документа со следующими параметрами:

Уникальный номер сертификата: 49 E7 30 21 00 00 00 00 0E 22
Дата начала срока действия сертификата: 30.08.2018 10:29:59
Дата окончания срока действия сертификата: 30.08.2019 10:29:59

Сведения о владельце сертификата:
Наименование* / Фамилия, имя и отчество (при наличии)**: Общество с ограниченной ответственностью "Ромашка"
ИНН / КИО*** 1234567890
Место нахождения: Липецкая обл, Чаплыгин г, Учительская ул, д. 1
Уполномоченное лицо****: Иванов Иван Иванович

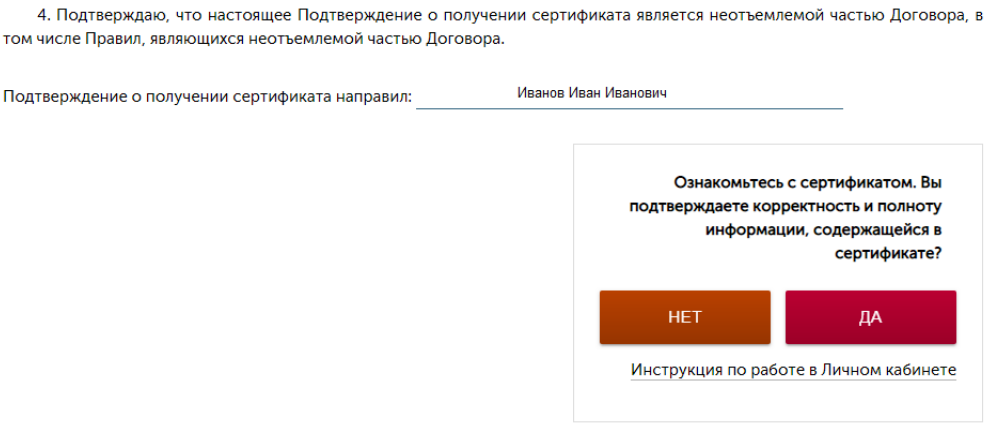
** Указывается в случае, если Клиент является юридическим лицом.*
*** Указывается в случае, если Клиент является физическим лицом.*
**** КИО – код иностранной организации.*
***** В случае если в сертификате Клиента – физического лица отсутствуют сведения о его Уполномоченном лице, в данном поле проставляется прочерк.*

Ключ проверки электронной подписи (открытый ключ):

```
04 81 80 f1 99 f3 e0 1d 18 eb 0d 49 97 96 ef a7 da b8 3d 24 ce
21 6c d9 db 5d 9c 14 35 e0 3f cb 7d 24 5f e9 e7 60 8a f4 d7 3c
0c 2a 08 ba c7 ac 24 e0 85 60 12 0a e3 b8 1b 71 0d 30 7b 49 24
35 d8 b6 96 0c 54 6a f9 8a 41 de 44 34 35 08 cf 6e 2f 40 d7 49
fd 62 c6 8a 4a f5 30 2a d7 ef 4f a3 06 3c b6 db 1b fe 17 30 5e ec
67 40 a0 b8 b5 43 a4 09 66 a4 5d 3d 6a e5 a8 ef d5 6d dc d5 be
e1 29 72 46
```

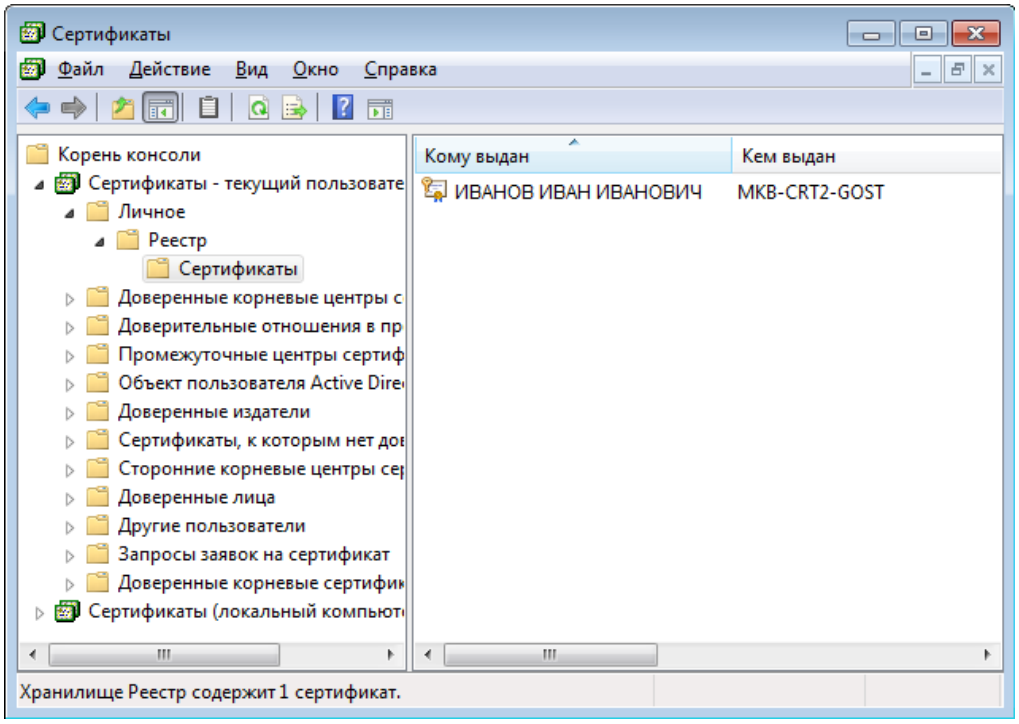
2. Подтверждаю, что содержащийся в сертификате ключ проверки электронной подписи используется для проверки подлинности электронной подписи Клиента на документе, полученном Банком посредством электронной системы «Ваш Банк Онлайн», а также иных сервисов электронного документооборота при наличии соответствующих договоров / соглашений, заключенных между Банком и Клиентом. Банк обеспечивает возможность использования Клиентом электронной подписи, удостоверенной сертификатом, не позднее рабочего дня, следующего за днем получения Банком настоящего Подтверждения о получении сертификата.

3. Подтверждаю, что ознакомлен с Правилами безопасного использования систем дистанционного банковского обслуживания и сервисов электронного документооборота, предоставляемых ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» клиентам – юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, в рамках соответствующих договоров (соглашений), размещенными на сайте Банка и являющимися неотъемлемой частью Правил обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).



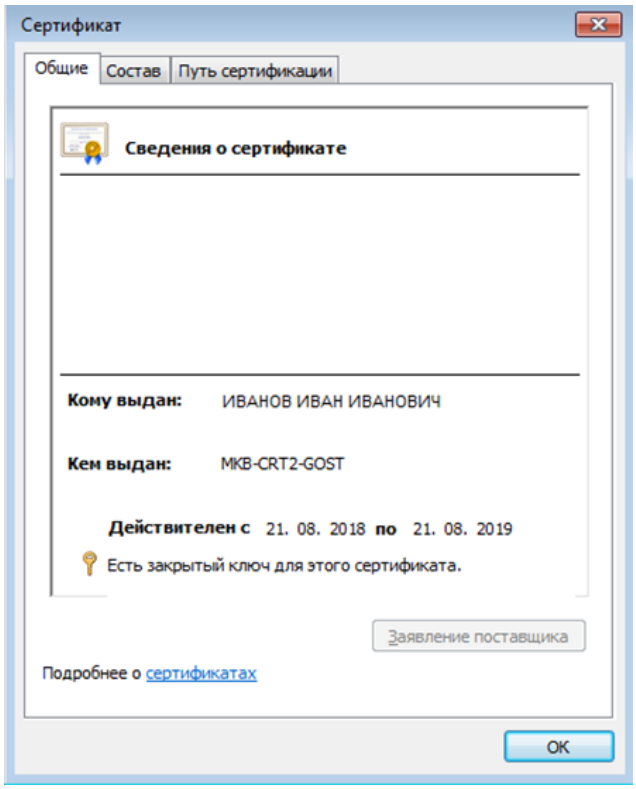
До отправки в Банк **«Подтверждения о получении сертификата»** проверьте сведения, указанные в нем. Для проверки сведений откройте файл сертификата, установленный на компьютере. Для этого выполните в меню Windows:
Пуск – Все программы – КРИПТО-ПРО – Сертификаты (или при помощи нажатия комбинации клавиш **«Win+R»** в окне введите команду **certmgr.msc** и нижмите **«Выполнить»**).
Необходимо перейти в папку **Сертификаты-текущий пользователь – Личное– Реестр – Сертификаты**.

Выберите нужный сертификат двойным нажатием мыши:

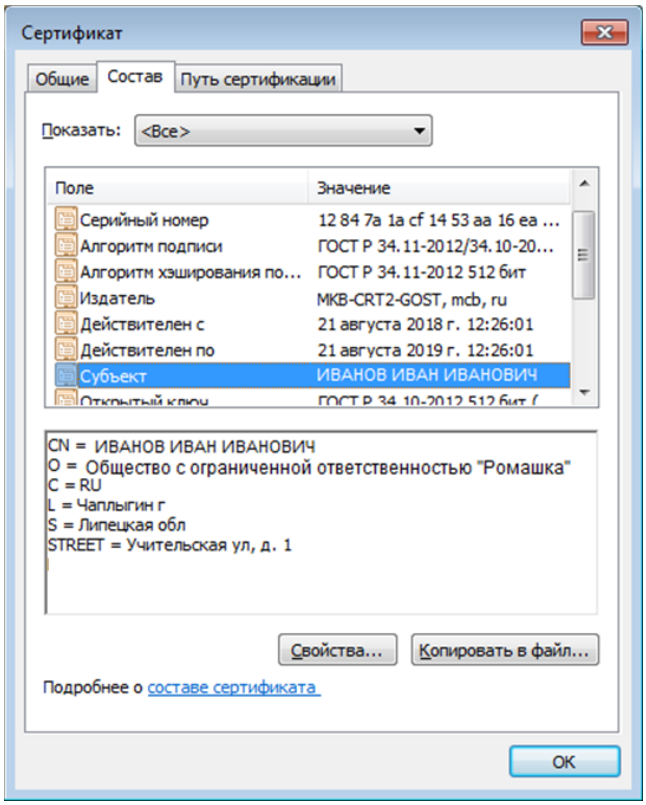


Необходимый сертификат можно определить по сведениям: кем выдан и срок действия (дата окончания срока действия)

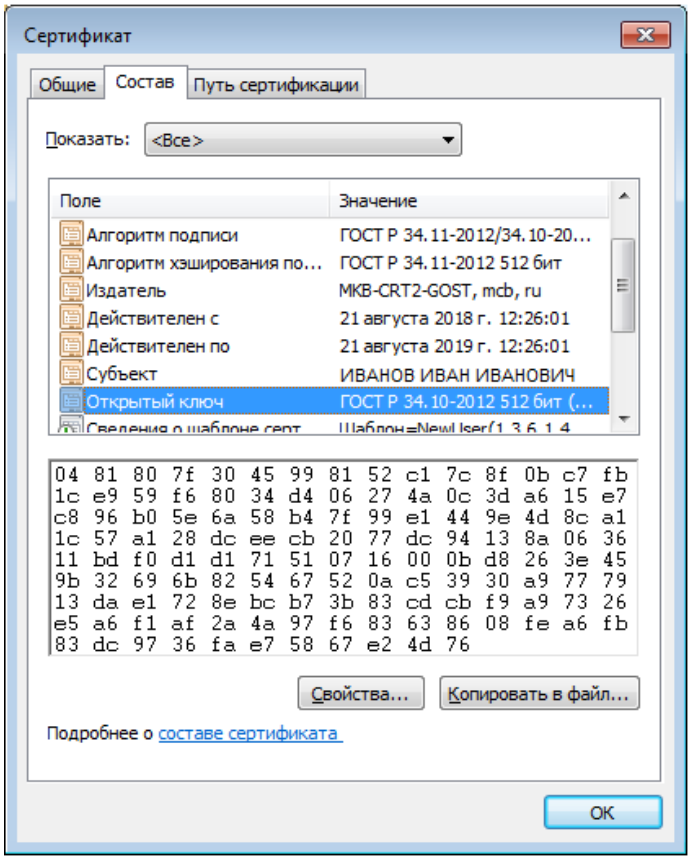
Откроется файл сертификата:



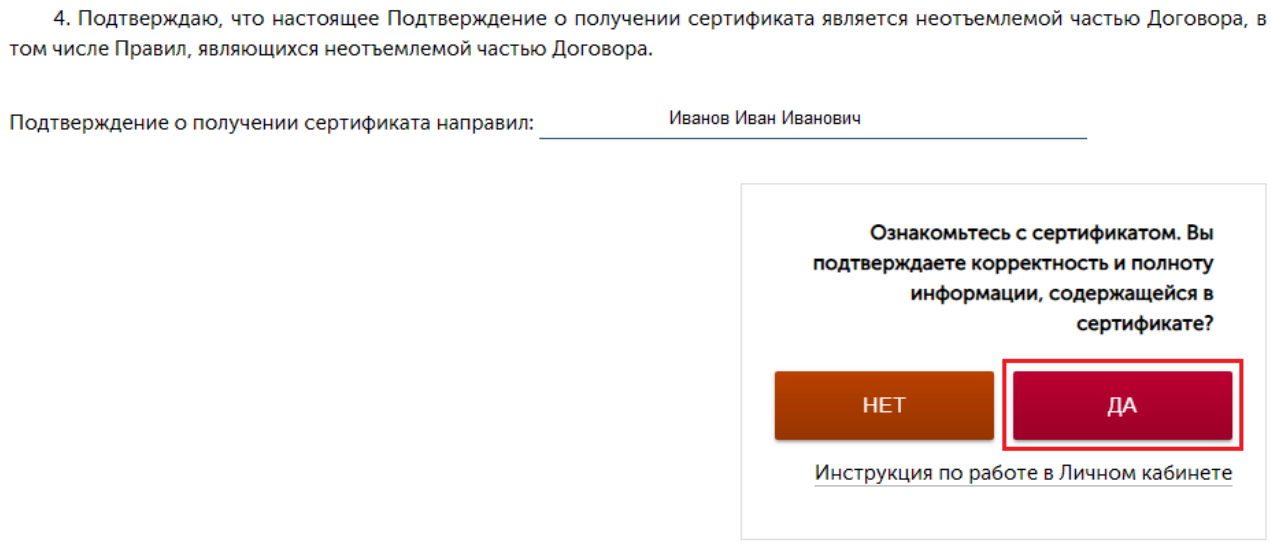
Для проверки серийного номера сертификата и срока его действия перейдите во вкладку **Состав.** Для проверки наименования Клиента, место нахождени и ФИО Уполномоченного лица во вкладке **Состав** выберите раздел **Субъект**:



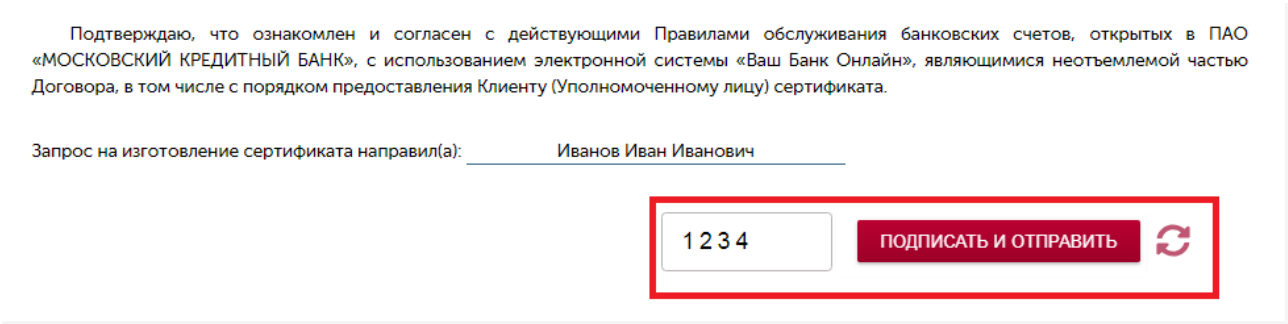
Для проверки ключа проверки ЭП (открытого ключа) во вкладке **Состав** выберите раздел **Открытый ключ**:



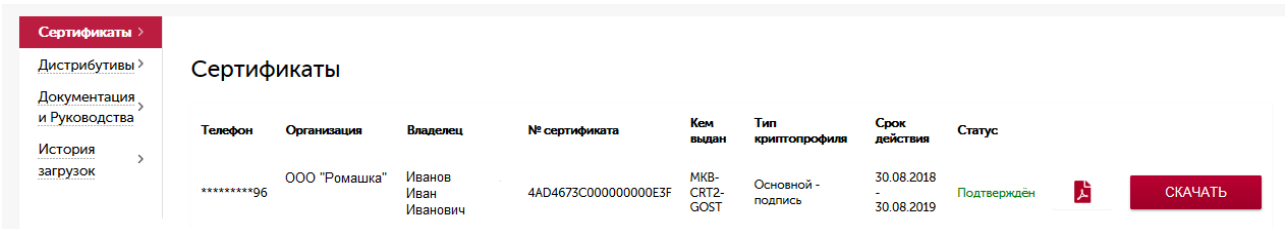
Если данные в **«Подтверждении о получении сертификата»** верны, подтвердите их корректность, нажав в форме документа **Да**:



В форме **«Подтверждение о получении сертификата»** откроется окно для подписания документа sms-кодом и отправки в Банк. Введите полученный sms-код и нажмите **Подписать и отправить:**

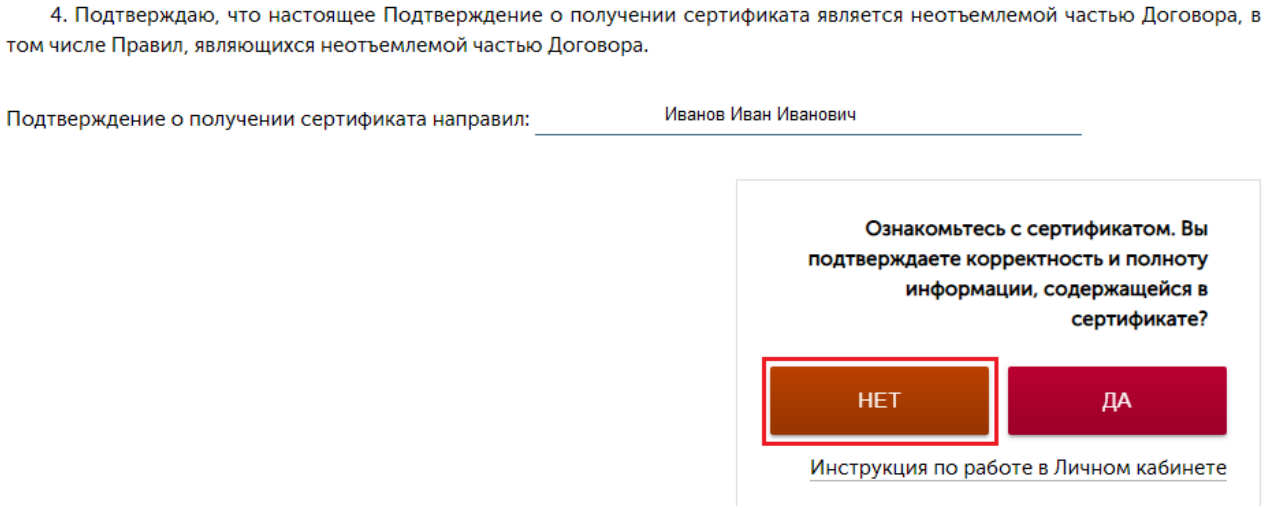


Если sms-код введен верно, документ «Подтверждение о получении сертификата» будет направлен в Банк. После успешной процедуры проверки «Подтверждения о получении сертификата» Банк активирует сертификат для работы в Системе и статус криптопрофиля изменится на **Подтвержден:**

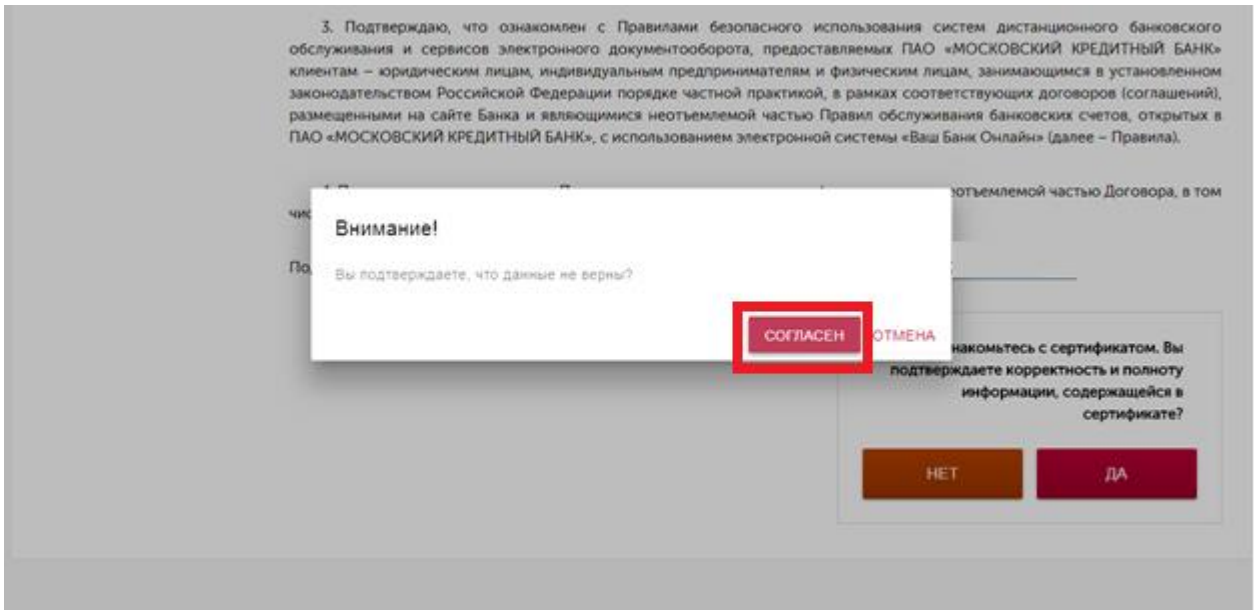


После выдачи Уполномоченному лицу первого сертификата и подключения его к Системе Банк направит Уполномоченному лицу для доступа к Системе:
- логин на адрес электронной почты Уполномоченного лица;
- инициализационный пароль на номер телефона Уполномоченного лица.

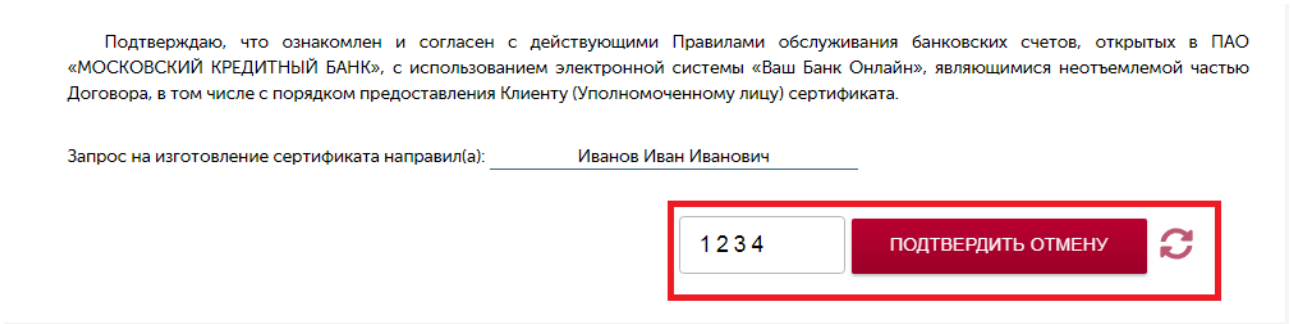
Если данные в «**Подтверждении о получении сертификата**» неверны, нажмите **Нет**:



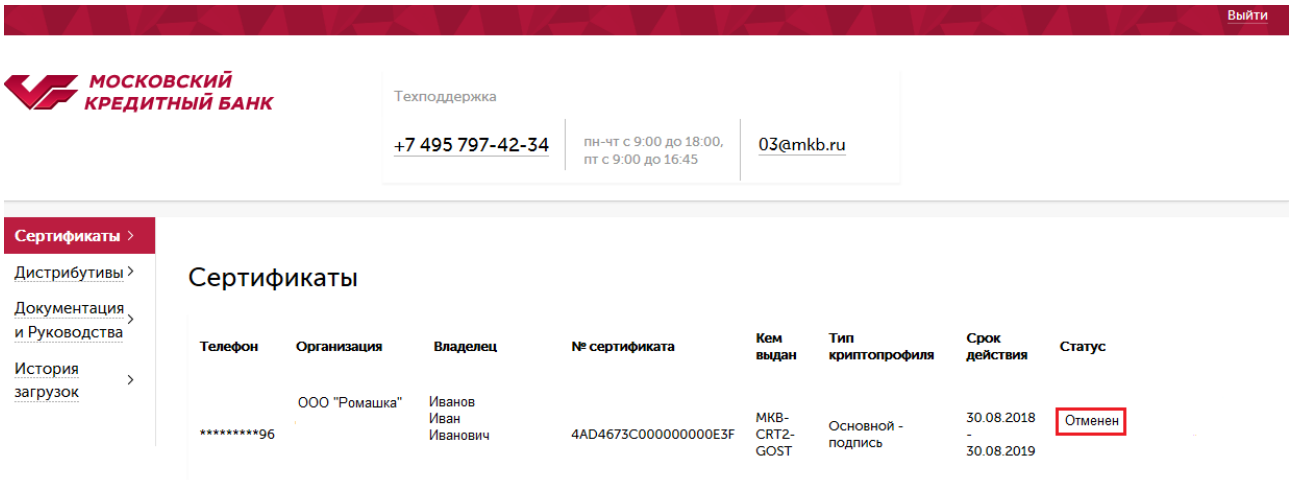
Подтвердите, что данные неверны, нажав **Согласен**:



В форме **«Подтверждение о получении сертификата»** отобразится окно для подтверждения отмены отправки документа в Банк. Введите полученный sms-код и нажмите **Подтвердить отмену**



Процедура получения сертификата будет прекращена и статус криптопрофиля изменится на Отменен:

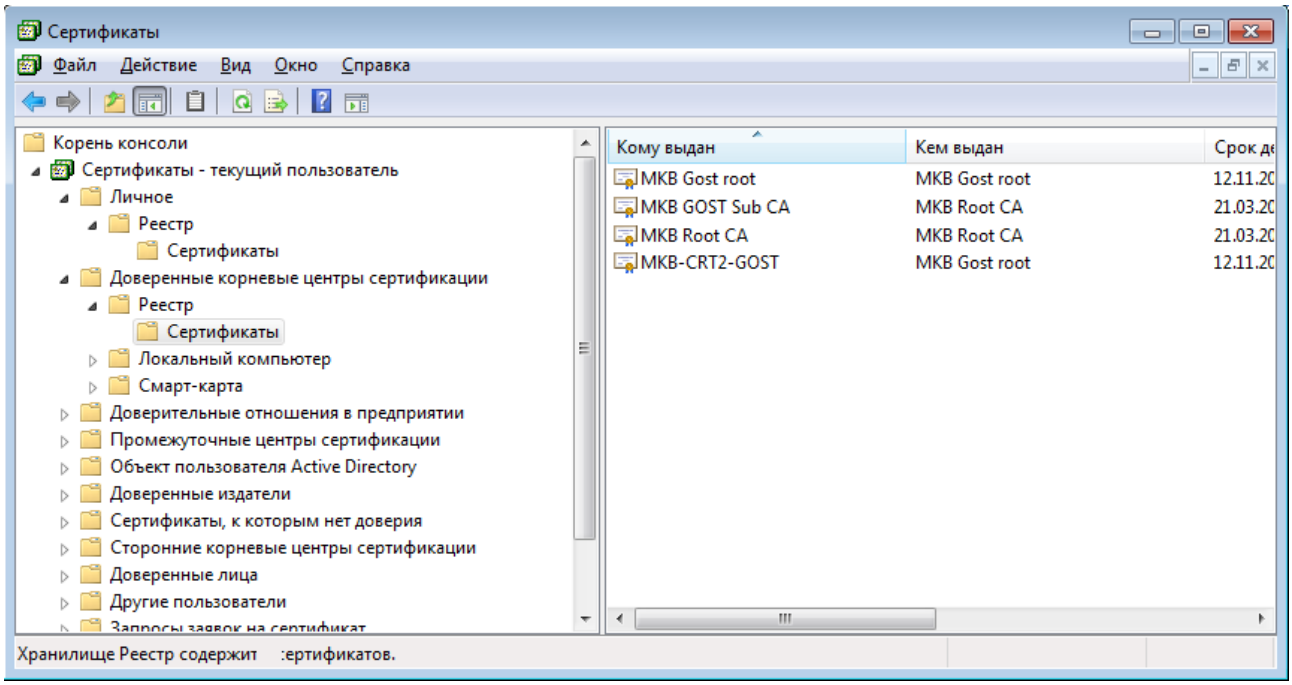


Сведения в документе «Подтверждение о получении сертификата» соответствуют сведениям, указанным Клиентом в Заявке и документе «Запрос на изготовление сертификата». В случае неверных сведений в документе «Подтверждение о получении сертификата» в отношении владельца сертификата (Клиента и его Уполномоченного

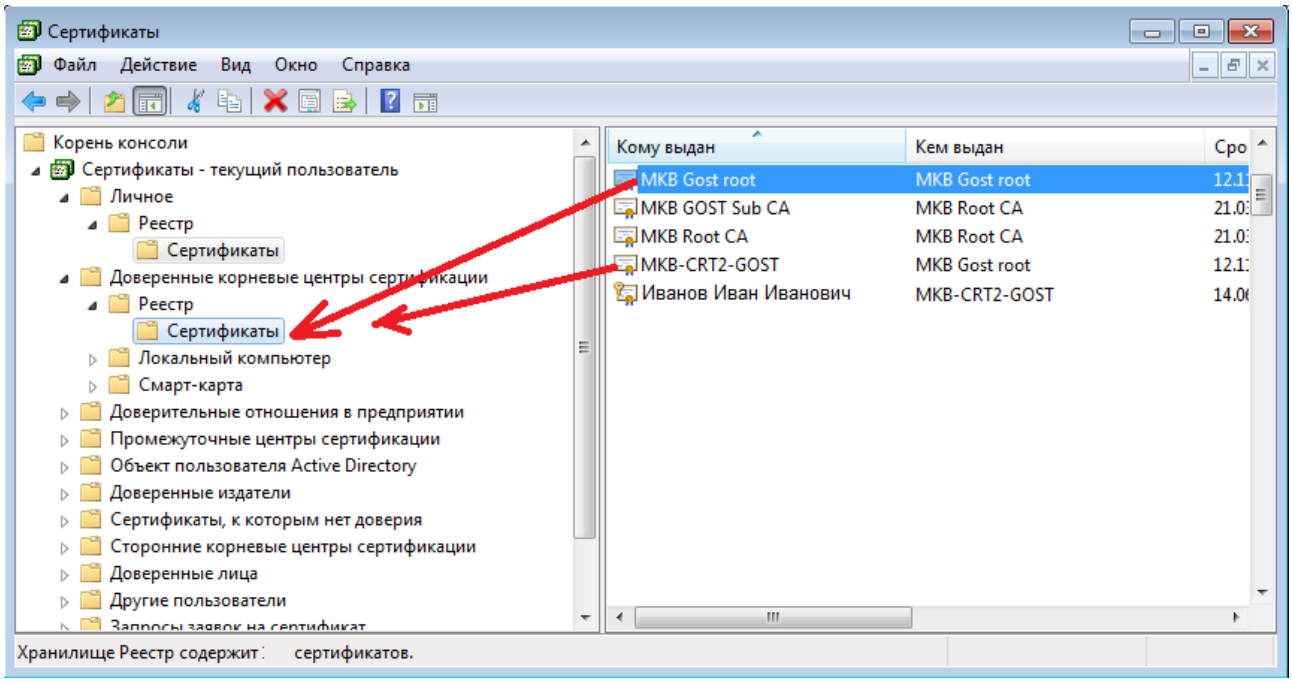
лица) Клиенту необходимо обратиться к клиентскому менеджеру / в обслуживающий дополнительный офис Банка и предоставить новую Заявку на данное Уполномоченное лицо, а также документы, подтверждающие изменение указанных ранее сведений. В случае неверных сведений в отношении ключа проверки ЭП Уполномоченному лицу необходимо обратиться в службу поддержки систем ДБО посредством Контакт-центра.

5. Перенос корневых сертификатов

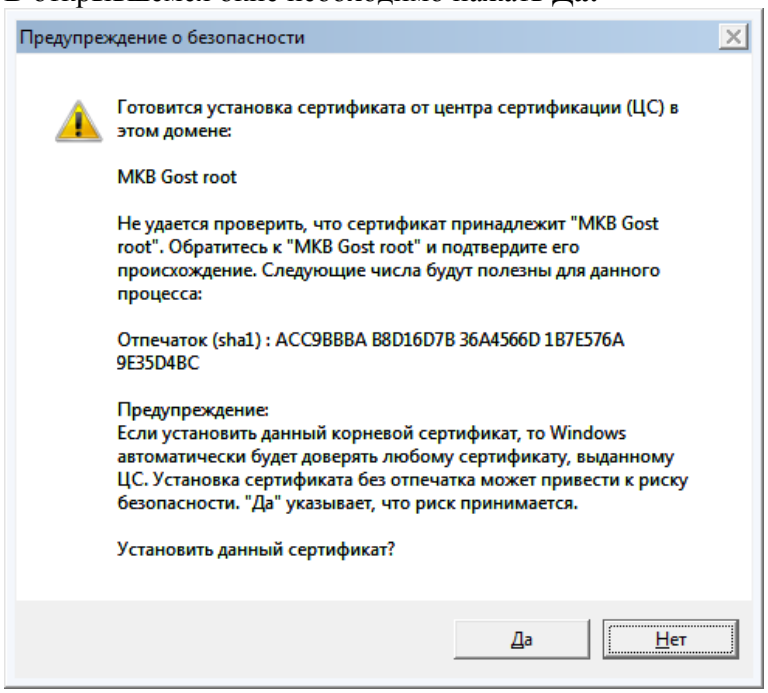
До корректной работы Системы может потребоваться перенос корневых сертификатов в раздел **Доверенные корневые центры сертификации**. Для этого выполните в меню Windows:
Пуск – Все программы – КРИПТО-ПРО – Сертификаты (или при помощи нажатия комбинации клавиш **«Win+R»** в окне введите команду **certmgr.msc** и нижмите **«Выполнить»**).
Необходимо одновременно раскрыть папки **Сертификаты-текущий пользователь – Личное – Реестр – Сертификаты** и **Сертификаты-текущий пользователь – Доверенные корневые центры сертификации – Реестр – Сертификаты**:



Далее из раздела **Сертификаты-текущий пользователь – Личное – Реестр – Сертификаты** необходимо перетянуть сертификаты **MKB Gost root** и **MKB-CRT2-GOST** в раздел **Сертификаты-текущий пользователь – Доверенные корневые центры сертификации – Реестр – Сертификаты**:

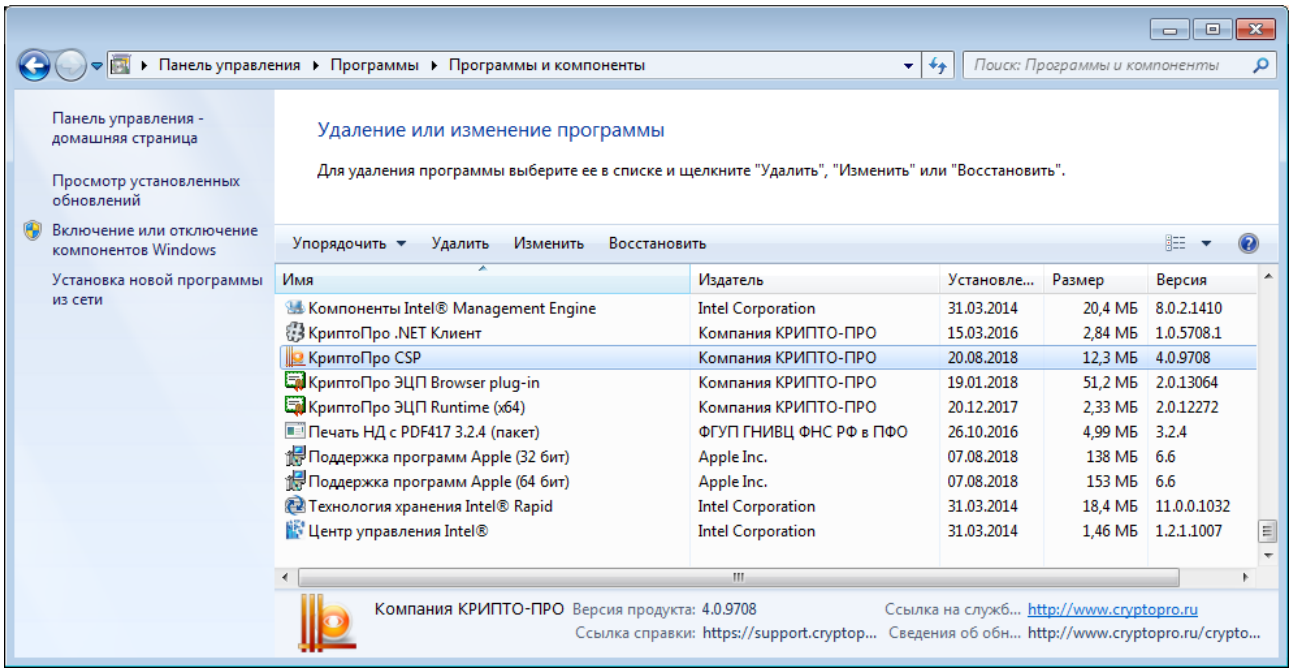


В открывшемся окне необходимо нажать **Да:**



6. Удаление СКЗИ «КриптоПро CSP»

Для корректного удаления «КриптоПро CSP» необходимо выполнить следующие действия:
– удалить установленную версию «КриптоПро CSP» через приложение **Установка и удаление программ** (меню Windows **Пуск – Панель Управления – Установка и удаление программ**) и перезагрузить компьютер:



– запустить утилиту очистки следов установки «КриптоПро CSP» **cspclean.exe** (утилиту можно скачать на сайте http://cryptopro.ru/downloads). После завершения работы утилиты следует перезагрузить компьютер.

Контакты службы поддержки систем дистанционного банковского обслуживания:
+7 495 797-42-34 (Контакт-центр Банка);
8 800 200-34-74 звонок по России бесплатный (Контакт-центр Банка);
03@mkb.ru