

**ИНСТРУКЦИЯ ПО ПОЛУЧЕНИЮ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА
ЭЛЕКТРОННОЙ ПОДПИСИ В УЦ IDC
(ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ)**

Оглавление

«IDC: УПРАВЛЕНИЕ КЛЮЧАМИ»	1
Создание запросов на получение сертификатов	1
1. Получение ключевых носителей в Удостоверяющем Центре	1
2. Инициализация нового ключевого носителя	2
3. Установка корневого сертификата	3
4. Создание запроса на сертификат	3
Оформление документов на создание и выдачу сертификатов	4
Загрузка сертификатов	5

Описание

«IDC: УПРАВЛЕНИЕ КЛЮЧАМИ»

Программа «IDC: Управление ключами» позволяет:

- устанавливать корневые сертификаты;
- создавать запросы на получение сертификатов открытых ключей электронной подписи (далее – «сертификаты»);
- загружать выданные сертификаты;
- отзывать (аннулировать) сертификаты.

Скачать и установить программу «IDC: Управление ключами» Вы можете по ссылке

<https://ca.idc.md/pki/certificate> (установите Microsoft.NET Framework версии 4.7.2 — доступно по ссылке <https://support.microsoft.com/ru-ru/help/4054530/microsoftnet-framework-4-7-2-offline-installer-for-windows>).

Создание запросов на получение сертификатов.

1. Получение ключевых носителей в Удостоверяющем Центре.

Для получения ключевых носителей для сотрудников компании необходимы следующие документы:

- выписка из ГРЮЛ, выданная не позднее, чем за 10 календарных дней до даты обращения в УЦ;
- паспорт лица (удостоверение личности), обладающего правом на представление интересов юридического лица без доверенности;
- справка из обслуживающего банка об открытии счетов.

В случае обращения за регистрацией иного лица, не указанного в выписке из ГРЮЛ, дополнительно предоставляется:

- паспорт (удостоверение личности) представителя заявителя.
- доверенность представителя.

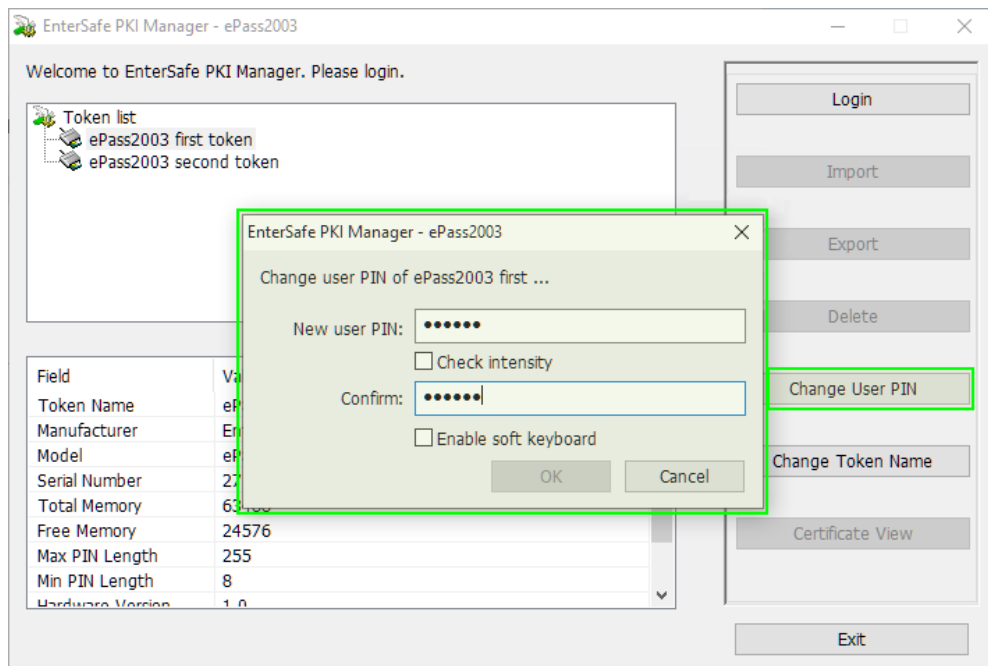
С этими документами уполномоченному представителю юридического лица необходимо обратиться к специалисту в Центр связи СЗАО «Интерднестрком» по адресу г. Тирасполь, ул. К. Маркса, 149. При себе необходимо иметь документ, удостоверяющий личность.

2. Инициализация нового ключевого носителя.

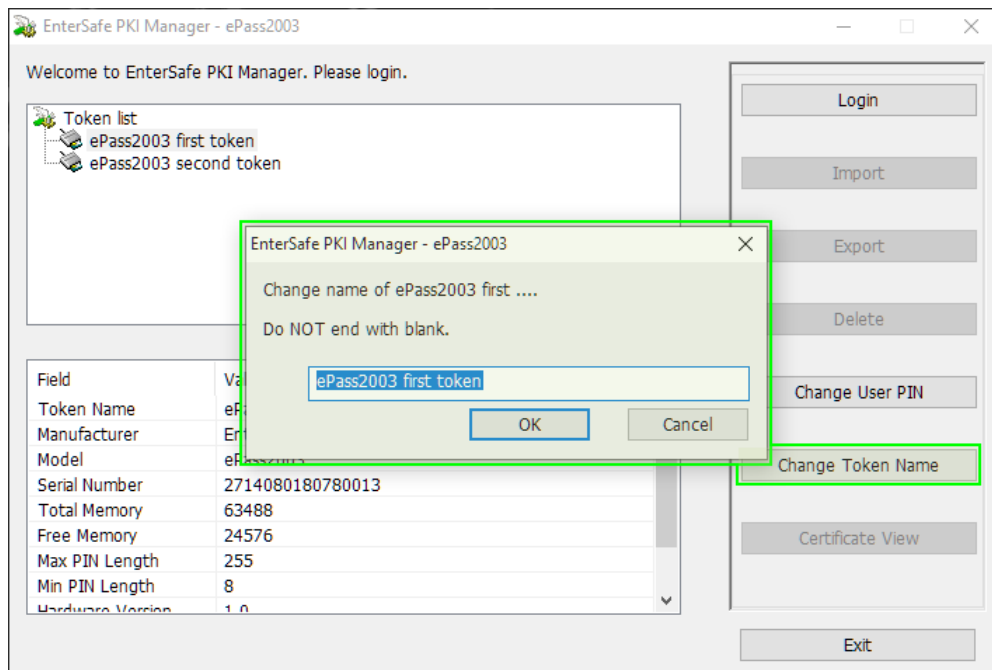
Инициализация — это активация и подготовка ключевого носителя к работе. Данную процедуру необходимо провести для каждого полученного ключевого носителя на рабочих местах сотрудников, получающих эти носители.

Для инициализации:

- подключите ключевой носитель к компьютеру
- установите программу «EnterSafe PKI Manager». Программу можно найти на ключевом носителе и на сайте УЦ, по адресу <https://ca.idc.md/pki/certificate>
- создайте ПИН-код пользователя (используется всегда перед началом работы с ключевым носителем)



- введите имя ключевого носителя (может быть любым, без пробелов в начале и конце)

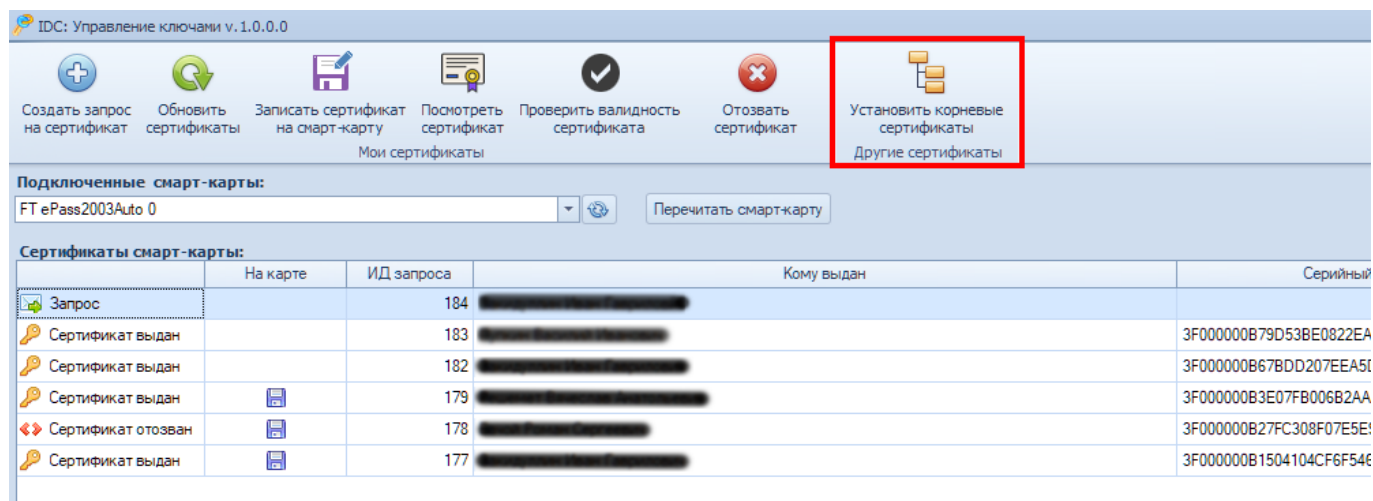


Внимание! Каждый сотрудник компании, получающий ключевой носитель, должен сформировать свой уникальный ПИН-код и держать его в секрете.

3. Установка корневого сертификата.

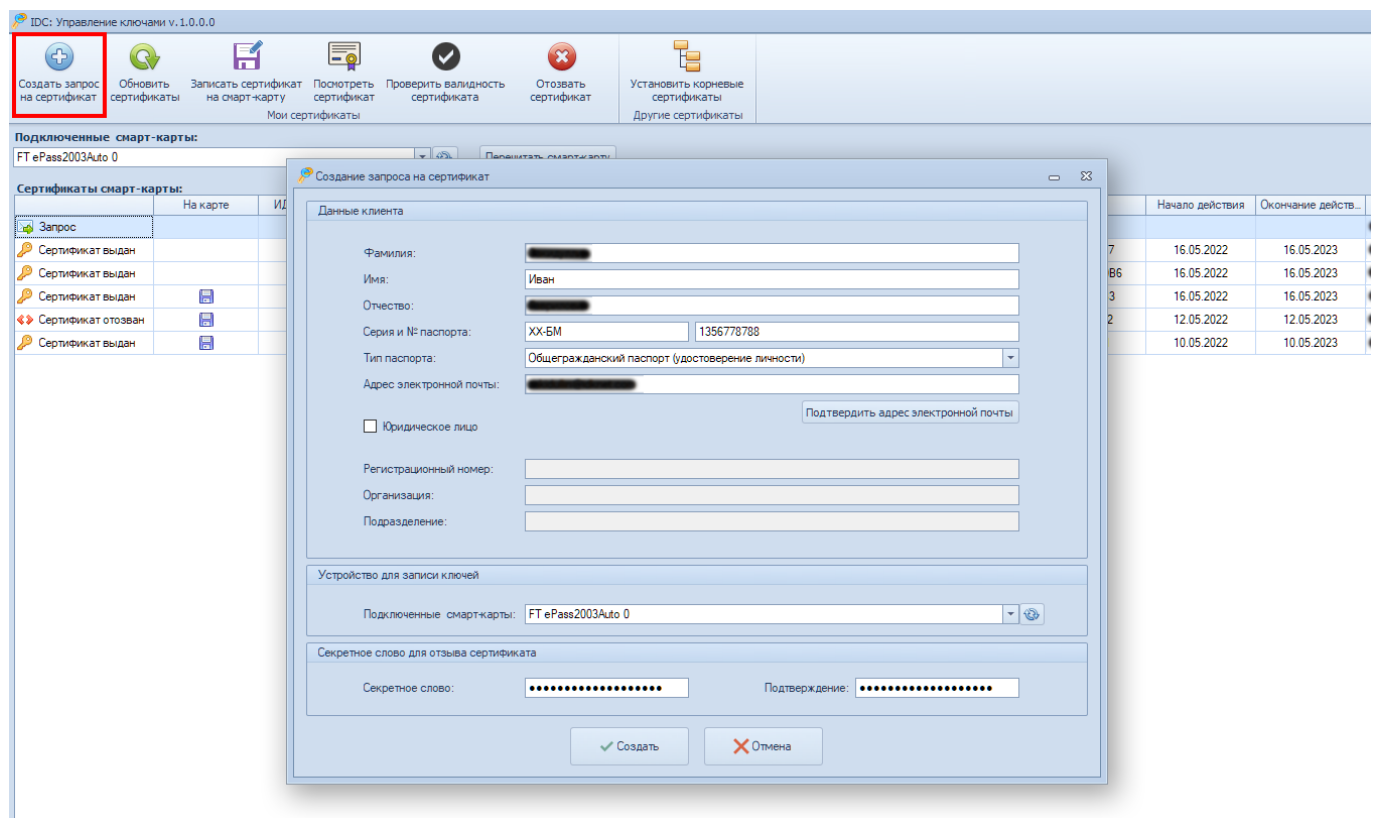
ВНИМАНИЕ! Запуск программы «IDC: Управление ключами» необходимо осуществлять с правами администратора.

При запуске программы «IDC: Управление ключами» производится проверка на установленные корневые сертификаты на рабочем месте пользователя, если они не найдены, запускается процесс установки. В случае если процесс установки корневого сертификата автоматически не запускается, нажмите кнопку «Установить корневые сертификаты» и подтвердите действие. Корневые сертификаты необходимы для того, чтобы установить доверие к Удостоверяющему Центру.



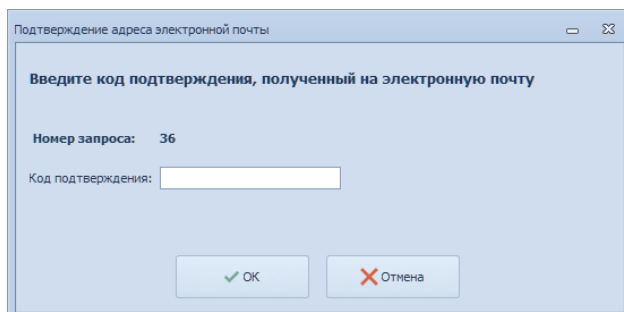
4. Создание запроса на сертификат.

Для создания запроса на получение сертификата открытого ключа нажмите на кнопку меню «Создать запрос на сертификат». Откроется окно «Создание запроса на сертификат».



Введите все необходимые данные в верхнем блоке полей ввода. В качестве типа документа выберите тот, который будет использоваться для регистрации и дальнейшего пользования. Установите признак «Юридическое лицо» и введите регистрационный номер, наименование Вашей организации и наименование подразделения в котором числится сотрудник.

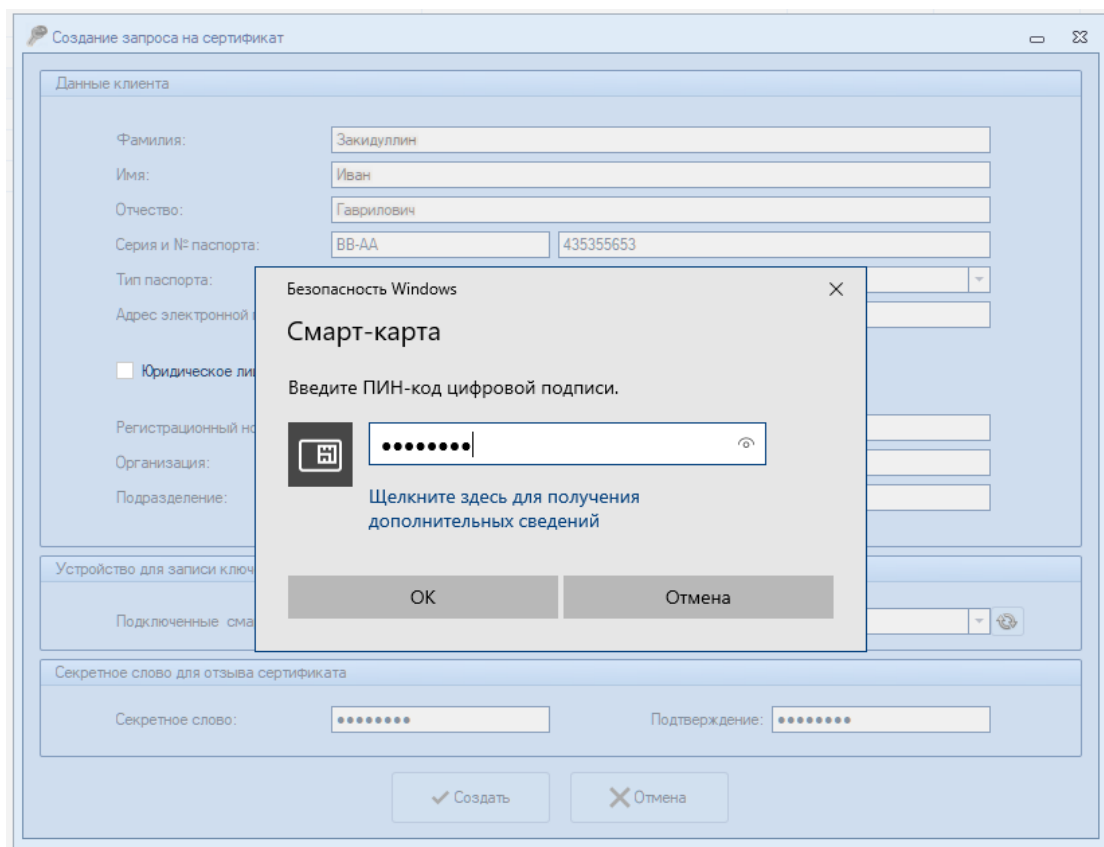
Если Вы заполнили поле «Адрес электронной почты», в этом случае его необходимо подтвердить. Для этого нажмите на кнопку «Подтвердить адрес электронной почты», а затем из письма, полученного на указанный адрес, скопируйте код подтверждения и вставьте его в соответствующее поле в открывшейся форме подтверждения.



Здесь также можно сменить ключевой носитель. По умолчанию будет выбран тот, который был активным при инициализации создания запроса на сертификат. Для того чтобы иметь возможность самостоятельно отозвать (аннулировать) сертификат в случае его компрометации, введите секретное слово и подтвердите его в соседнем реквизите. Требования к секретному слову — длина не менее шести любых символов. Секретное слово должно быть засекречено и быть известно только владельцу сертификата. После того, как все реквизиты заданы, перепроверьте правильность их заполнения, так как изменить их позже будет нельзя. Нажмите на кнопку «Создать».

Для доступа к внутреннему хранилищу ключевого носителя программа запросит ввести ПИН-код, который Вы создали ранее, при инициализации ключевого носителя.

Данная процедура прodelывается для каждого сотрудника компании, получающего сертификат, при подключенном ключевом носителе данного сотрудника к персональному компьютеру на его рабочем месте.



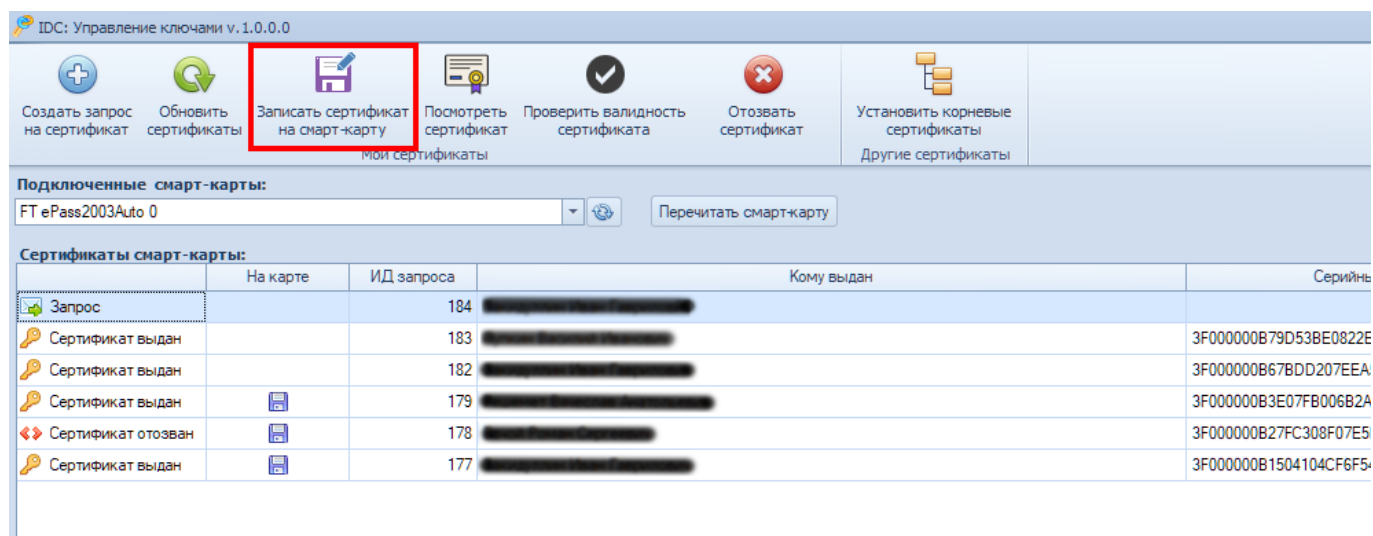
Оформление документов на создание и выдачу сертификатов.

После создания запросов на сертификаты для всех сотрудников, кому выданы ключевые носители, уполномоченный представитель юридического лица с документом, удостоверяющим личность, должен обратиться к специалисту в Центр связи СЗАО «Интерднестрком» по адресу г. Тирасполь, ул. К. Маркса, 149 для оформления всех необходимых документов, создания и выдачи сертификатов.

Загрузка сертификатов.

Уведомления об успешной выдаче сертификатов придут на адреса электронной почты сотрудников, которые были указаны при создании запросов на сертификаты.

Для загрузки сертификата на ключевой носитель подключите его к компьютеру и запустите программу «IDC: Управление ключами». **Внимание! При записи сертификата в качестве активного ключевого носителя должен быть выбран тот носитель, который был активен при подаче запроса на получение сертификата. В противном случае запись сертификата на носитель не сможет быть произведена. При этом будет выдано соответствующее сообщение.** Программа выдаст запрос на ввод ПИН-кода для доступа к внутреннему хранилищу ключевого носителя. Введите Ваш ПИН-код. Нажмите на кнопку «Записать сертификат на смарт-карту». После успешной записи сертификата во внутреннее хранилище ключевого носителя в списке запросов в колонке «На карте» будет отображена пиктограмма, подтверждающая это. **Внимание! Если после ввода ПИН-кода для доступа к ключевому носителю при его подключении к компьютеру прошло достаточно много времени, программа может повторно запросить ввод ПИН-кода.**



	На карте	ИД запроса	Кому выдан	Серийный номер
Запрос		184		
Сертификат выдан		183		3F000000B79D53BE0822E
Сертификат выдан		182		3F000000B67BDD207EEA
Сертификат выдан	📄	179		3F000000B3E07FB006B2A
Сертификат отозван	📄	178		3F000000B27FC308F07E5
Сертификат выдан	📄	177		3F000000B1504104CF6F5