

Инструкция по созданию и применению электронной цифровой подписи в Adobe Acrobat/Reader.


О цифровых подписях

Цифровая подпись, как и обычная подпись, шариковой ручкой, идентифицирует лицо, подписавшее документ. Но, в отличие от ручной, цифровую подпись очень сложно подделать, так как она содержит зашифрованную, уникальную для подписывающего информацию. Получатели документа могут легко проверить подпись, а также определить, был ли документ изменен после того, как он был подписан.

Чтобы подписать документ, необходимо создать в Acrobat® или Reader® цифровое удостоверение с собственной подписью. В цифровом удостоверении содержится закрытый ключ, а также сертификат с открытым ключом и другими данными. Закрытый ключ используется для создания цифровой подписи. Сертификат — это учетные данные, которые автоматически применяются к подписанному документу. Цифровая подпись проверяется при открытии документа получателями.

При создании цифровой подписи Acrobat при помощи хэш-алгоритма производит генерацию обработки сообщения, которое затем зашифровывается с использованием закрытого ключа. Acrobat встраивает зашифрованный хэш сообщения в документ PDF, сведения о сертификате, изображение подписи и версию документа при его подписании.


Создание цифрового удостоверения с собственной подписью

1. Выполните одно из следующих действий:
 - В приложении Acrobat выберите «Инструменты» — «Подпись и сертификация» — «Дополнительные возможности подписи и сертификации» — «Параметры защиты».
 - В приложении Reader выберите «Редактирование» — «Защита» — «Параметры защиты».
2. Выберите слева «Цифровые удостоверения» и нажмите кнопку «Добавить удостоверение» .
3. Выберите пункт «Новое удостоверение, которое нужно создать» и нажмите «Далее».
4. В качестве места хранения цифрового удостоверения, выберите «Новый файл цифровых удостоверений PKCS#12» и нажмите кнопку «Далее».

Примечание. Информация о цифровом удостоверении сохранится в файле с расширением .pfx в Windows и .p12 в Mac OS. Эти файлы могут использоваться в обеих операционных системах. Если файл переносится из одной операционной системы в другую, программа Acrobat сможет его распознать.


5. Заполните предложенные поля по следующему шаблону, и нажмите «Далее»:
 - Имя – Ваше имя;
 - Подразделение – необходимо указать свою должность;
 - Организация;
 - Адрес электронной почты – свой адрес электронной почты;
 - Страна/Регион – «RU – РОССИЙСКАЯ ФЕДЕРАЦИЯ»
 - Алгоритм ключа – «1024-bit RSA»
 - Использовать цифровое удостоверение для – «Цифровых подписей и шифрования данных»
6. Введите пароль для файла цифрового удостоверения. При нажатии каждой клавиши указатель надежности пароля оценивает пароль и указывает степень надежности, используя цветовые шаблоны. Подтвердите свой пароль и нажмите «Готово». Ваше цифровое удостоверение сформировано.

Экспорт сертификата электронной цифровой подписи в файл

1. Откройте окно «Параметры защиты» (см. первый пункт раздела «Создание цифрового удостоверения с собственной подписью»).
2. Выберите слева «Цифровые удостоверения» и нажмите кнопку «Экспорт» .
3. В открывшемся окне «Файл обмена данными – параметры экспорта» выберите пункт «Сохранить данные в файле» и нажмите «Далее»
4. Введите имя файла, выберите папку и нажмите кнопку «Сохранить».

5. Сохраненный файл .fdf содержит информацию об открытом ключе Вашей электронной цифровой подписи, этот файл необходимо передать представителю компании ООО «Синтек»

Формирование Сертификата электронной цифровой подписи согласно Приложению №3 к Соглашению о применении электронной цифровой подписи.

1. Откройте окно «Параметры защиты» (см. первый пункт раздела «Создание цифрового удостоверения с собственной подписью»).
2. Выберите слева «Цифровые удостоверения» и нажмите кнопку «Сведения о сертификате» .
3. В открывшемся окне выберите вкладку «Подробно».
4. Скопируйте данные Сертификата из нижнего окна вкладки «Подробно» в соответствующие поля формы Сертификата электронной цифровой подписи (Приложение №3 к Соглашению о применении электронной цифровой подписи), распечатайте в двух экземплярах, подпишите собственноручной подписью и передайте один экземпляр представителю компании ООО «Синтек», второй экземпляр храните у себя.

Настройка внешнего вида электронной цифровой подписи

1. Отсканируйте и сохраните в файл изображение собственноручной подписи.
2. Выберите пункт меню «Редактирование» – «Установки».
3. В открывшемся окне выберите категорию «Защита».
4. В области «Внешний вид» нажмите кнопку «Создать...».
5. В диалоговом окне «Настройка вида подписи» введите заголовок вида подписи. Перед использованием подписи ее можно выбрать с помощью этого имени. Поэтому рекомендуется указывать краткое и информативное название.
6. В области «Настройка графики» выберите пункт «Импортированную графику», нажмите на кнопку «Импортировать графику из: «Файла...».
7. В открывшемся окне нажмите кнопку «Обзор...» и выберите файл с изображением собственноручной подписи, нажмите кнопку «Ок».
8. В области «Настройка текста» уберите все галочки.
9. В области «Образец» Вы должны увидеть только изображение собственноручной подписи, нажмите кнопку «Ок».

Импорт информации о сертификате в Adobe Acrobat/Reader

1. Загрузите необходимый файл с сертификатом (.fdf), с официального сайта компании ООО «Синтек», и откройте его (выполните двойной щелчок левой кнопкой мыши).
2. В открывшемся окне «Файл обмена данными – импорт контакта» нажмите кнопку «Доверие контакта».
3. В окне «Настройка импорта контакта» установите галочку «Используйте этот сертификат в качестве надежного корневого сертификата», а также галочки «Сертифицированные документы», «Динамическое содержание», «Встроенный сценарий JavaScript с высоким уровнем полномочий», «Привилег. сист. операции (работа в сети, печать, доступ к файлам и т.д.)» и нажмите «Ок».
4. Убедитесь что импорт прошел удачно и нажмите кнопку «Ок».
5. В окне «Файл обмена данными – импорт контакта» нажмите кнопку «Закреть». Теперь при открытии документа PDF, наведя курсор на изображение подписи можно удостовериться в действительности электронной подписи сотрудника компании ООО «Синтек», Ваша личная электронная подпись также может быть проверена на ее действительность получателем электронного документа.