

РИАМС ПроМед
Работа с электронной цифровой
подписью
Инструкция пользователя

© РИАМС ПроМед, 2017
Работа с электронной цифровой подписью
Инструкция пользователя
Версия документа I.00.066.133-001

Официальный сайт: <http://swan.perm.ru>
Справочная информация: <http://promed.promedweb.ru/wiki/khak/wiki/Содержание>



В зависимости от версии работа Системы может отличаться от приведенного описания. За более актуальной информацией обратитесь к справочной системе

© 2009-2017 РИАМС ПроМед. Все права защищены.

Содержание

Термины и сокращения	4
1 Назначение и порядок применения	5
1.1 Поддерживаемые типы ЭП.....	5
1.2 Общие положения.....	5
1.3 Используемый формат ключей и ЭП	6
2 Установка плагина	7
3 Загрузка сертификатов пользователей	8
4 Использование ЭЦП при работе с документами.....	9

Термины и сокращения

- **Смарт-карты:** пластиковые карты со встроенной микросхемой (англ. integrated circuit card, ICC — карта с интегрированными электронными цепями).
- **Кард-ридер:** устройство для работы со смарт-картами.
- **USB-ключ:** устройство, объединяющее блок данных смарт-карты и необходимое для работы с блоком данных оборудование в едином корпусе, подключающееся в разъем USB.
- **ПК.** Персональный компьютер пользователя.
- **СОДС:** Средство обеспечения доверенного сеанса – устройство, обеспечивающее полноценную криптографическую защиту информации во время доверенного сеанса связи (ДСС).
- **УЭК:** Универсальная Электронная Карта — российская пластиковая карта, объединяющая в себе идентификационное и платёжное средство.
- **ЭЦП** - электронная цифровая подпись.

1 Назначение и порядок применения

Служба поддержки инфраструктуры электронной подписи «Промед» (СПИ ЭП «Промед») предназначена для присваивания учетным документам электронной подписи, и предоставляет единый интерфейс для осуществления идентификации и считывания личных данных со смарт-карт разных форматов.

1.1 Поддерживаемые типы ЭП

- карта УЭК.
- карта электронного полиса (ЭП).
- Башкирская Социальная Карта.
- USB токен СОДС «Марш!».
- электронные USB-ключи и смарт-карты eToken Pro, eToken ГОСТ.
- электронные USB-ключи Rutoken и Rutoken ЭЦП.
- программный токен ЛИССИ LS11SW.
- jaCarta.
- Kaztoken.
- PKCS#12 ГОСТ.
- PKCS#12 RSA.

Одновременно могут быть доступны несколько устройств. Например «Марш!» врача и УЭК, УЭК и карта электронного полиса и т.д.

1.2 Общие положения

ЭП — реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭП и позволяющий идентифицировать владельца, а также установить отсутствие искажения информации в электронном документе.

ЭП представляет собой некую последовательность символов, которая формируется в результате определенного преобразования исходного документа (или любой другой информации) при помощи специального программного обеспечения. ЭП добавляется к исходному документу, любое изменение исходного документа делает эту ЭП недействительной. ЭП является уникальной для каждого документа и не может быть перенесена на другой документ. Невозможность подделки ЭП обеспечивается значительным количеством математических вычислений, необходимых для её подбора. ЭП является на сегодняшний день законодательно оформленной и юридически значимой процедурой обмена защищенными данными через телекоммуникационные

каналы связи, в частности, Интернет. Согласно Федеральному закону № 149-ФЗ, электронное сообщение, подписанное ЭП, признается равнозначным документу, подписанному собственноручно, если иным нормативным актом не предусмотрена обязательность бумажного носителя. Для шифрования и дешифрования сообщения используется пара ключей – Открытый и Закрытый ключи – которые используются для формирования ЭП.

1.3 Используемый формат ключей и ЭП

За основу формата хранения ключей и ЭЦП приняты форматы, используемые на портале Электронного Правительства РФ (<http://www.gosuslugi.ru/pgu/eds>).

Вид электронной подписи: отсоединенная. Отсоединенная ЭП содержится в отдельном файле.

Формат электронной подписи: xml-dsig (<http://www.w3.org/TR/xmlldsig-core/>).

Формат хранения открытого ключа: в составе сертификата X.509.

Алгоритмы формирования и проверки ЭП реализованы в соответствии с ГОСТ Р 34.10-2001.

Комплект ЭЦП при выдаче ее удостоверяющим центром выглядит следующим образом:

- Сертификат ключа пользователя (открытый ключ на бумажном носителе).
- Закрытый и открытый ключи на защищенном носителе — портативном устройстве, выполненном в форме USB-брелока, обеспечивающем хранение конфиденциальной ключевой информации и аутентификацию пользователя.

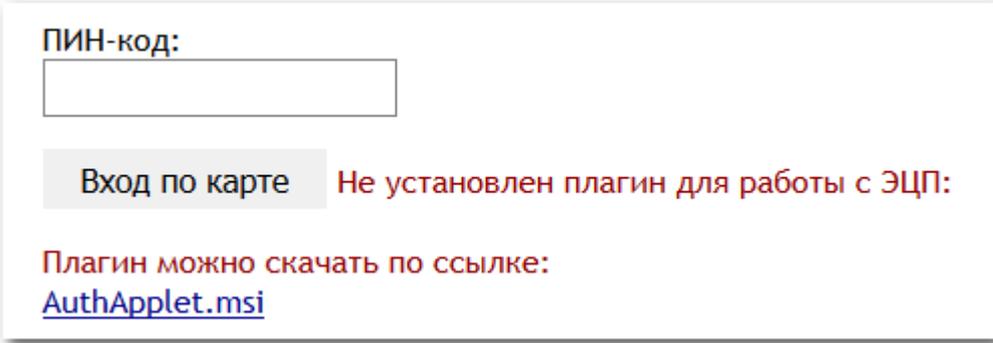
2 Установка плагина

Установка СПИ ЭП выполняется администратором системы. Порядок установки и настройки компонентов приведен в документе «Инструкция администратора по развертыванию службы поддержки инфраструктуры ЭП РИАМС».

На клиентских машинах, на которых установлена Система дополнительно необходимо установить плагин для возможности работы с использованием ЭП.

Порядок установки:

1. Запустите интернет-обозреватель.
2. Откройте страницу авторизации в Системе.
3. Нажмите кнопку **Вход по карте**. Отобразится сообщение с предложением установить плагин.



ПИН-код:

Вход по карте Не установлен плагин для работы с ЭЦП:
Плагин можно скачать по ссылке:
[AuthApplet.msi](#)

4. Запустите установку плагина, следуйте указаниям установщика.
5. По завершении установки перезапустите интернет-браузер. Убедитесь, что плагин не заблокирован средствами защиты интернет-браузера. В случае блокировки разрешите установку и использование плагина.

После успешной установки пользователю системы будет доступна авторизация с использованием поддерживаемых типов устройств и подписание учетных документов.

3 Загрузка сертификатов пользователей

Для учетной записи пользователя должен быть загружен сертификат в систему:

1. Откройте форму настройки параметров учетной записи пользователя **Сервис – Пользователи**.
2. Выберите в списке учетную запись, для которой следует загрузить сертификат ключа пользователя.
3. Откройте форму редактирования параметров учетной записи с помощью кнопки **Изменить**. Если учетная запись пользователя не создана, следует добавить ее в Систему
4. Нажмите кнопку **Сертификаты**. Отобразится форма загрузки сертификатов пользователя. Сертификат должен быть в формате PKCS7.
5. Для добавления сертификата пользователя нажмите кнопку **Добавить**.
6. Укажите путь к файлу-сертификату, нажмите кнопку **Загрузить**. Сертификат будет загружен. Файл сертификата предоставляется удостоверяющим центром, при выдаче электронного ключа.
7. Нажмите кнопку **Сохранить** для сохранения внесенных изменений.
8. Для применения настроек необходимо выйти из системы и авторизоваться под учетной записью пользователя, для которой были добавлены настройки.

4 Использование ЭЦП при работе с документами

Использование электронной цифровой подписи используется при работе с учетными документами.

При работе с учетным документом пользователь может:

- подписать документ.
- верифицировать документ (проверить наличие электронной подписи).
- просмотреть список версий.
- отменить подпись.

 **Важно:** Для использования функции usb-ключ должен быть подключен к ПК пользователя.

При нажатии кнопки **Подписать** отобразится форма для ввода пин-кода пользователя usb-ключа. Пин-код предоставляется пользователю вместе с usb-ключом.

Отмена подписи доступна только пользователю, который подписал документ.

 **Примечание** – Если реестр находится в списке «В работе» или «К оплате», то с подписанного случая, находящегося в реестре, можно снять подпись (кнопка есть, подпись снимается). Если реестр находится в списке «Оплаченные», то кнопка «Снять подпись» отсутствует, подпись снять нельзя.