Использование электронной подписи в системе межведомственного электронного взаимодействия

Докладчик: Начальник отдела информационной безопасности ГБУ СО «СОЦИ» Платонов Евгений Леонидович

14 марта 2012 г.
г. Южно-Сахалинск.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Простая электронная подпись

электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом

Усиленная электронная подпись

Усиленная неквалифицированная ЭП создается с применением средств криптографии и позволяет определить не только автора документа, но и проверить документ на наличие изменений.

Усиленная квалифицированная ЭП создается с применением сертификата ЭП Удостоверяющего центра, предназначена для организации юридически значимого электронного документооборота.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Применение квалифицированной электронной подписи

1. Электронная отчетность в контролирующие органы и внебюджетные фонды. ФНС, ПФР, ФСС, Росстат.

2. Электронные торги на федеральных (при размещении госзаказа) и коммерческих электронных торговых площадках.

3. Предоставление счетов-фактур в электронном виде.

4. Обмен документами, заверенными электронной подписью, при взаимодействий организаций (договоры, акты и т.д.)

5. Арбитражные процессы при банкротстве организаций и продаже имущества при помощи арбитражных управляющих.

6. При межведомственном электронном взаимодействии при предоставлении государственных и муниципальных услуг.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Постановление Правительства Российской Федерации от 9 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой»

1. При межведомственном электронном взаимодействии изготовление ключей ЭП осуществляется по обращению участников межведомственного электронного взаимодействия в удостоверяющий центр, аккредитованный в порядке, установленном Федеральным законом «Об электронной подписи». Изготовление ключей ЭП осуществляется с использованием средств ЭП в соответствии с требованиями, установленными ФСБ РФ.
2. Выдача квалифицированного сертификата ключа проверки ЭП осуществляется лицу, которое в установленном порядке наделено полномочиями по подписанию электронных документов ЭП
3. Средства ЭП должны соответствовать требованиям к обеспечению совместимости средств электронной подписи при организации электронного взаимодействия органов исполнительной власти и органов местного самоуправления между собой.
4. Подписанный ЭП документ должен иметь метку времени.
5. Подписанные ЭП документы, передаваемые участниками межведомственного электронного взаимодействия друг другу, проходят процедуру признания ЭП.

Постановление Правительства Российской Федерации от 9 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой»

6. ЭП признается действительной при одновременном соблюдении п.1,3,4 статьи 11 Федерального закона « Об электронной подписи».
7. Участнику межведомственного электронного взаимодействия, направившему электронный документ, который подписан ЭП, признанной недействительной, направляется уведомление об отказе в приеме к обработке такого документа.
8. Сертификат ЭП действует с момента выдачи и прекращает свое действие в соответствии с условиями, предусмотренными частью 6 статьи 14 Федерального закона « Об электронной подписи»
9. Действие сертификата, выданного участнику межведомственного взаимодействия на имя его уполномоченного лица, прекращается в следующих случаях:

- при смене уполномоченного лица;
- в случае нарушения конфиденциальности ключа ЭП;
- в случае возникновения обстоятельств, не позволяющих уполномоченному лицу правомерно использовать ЭП и средства ЭП.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Удостоверяющие центры

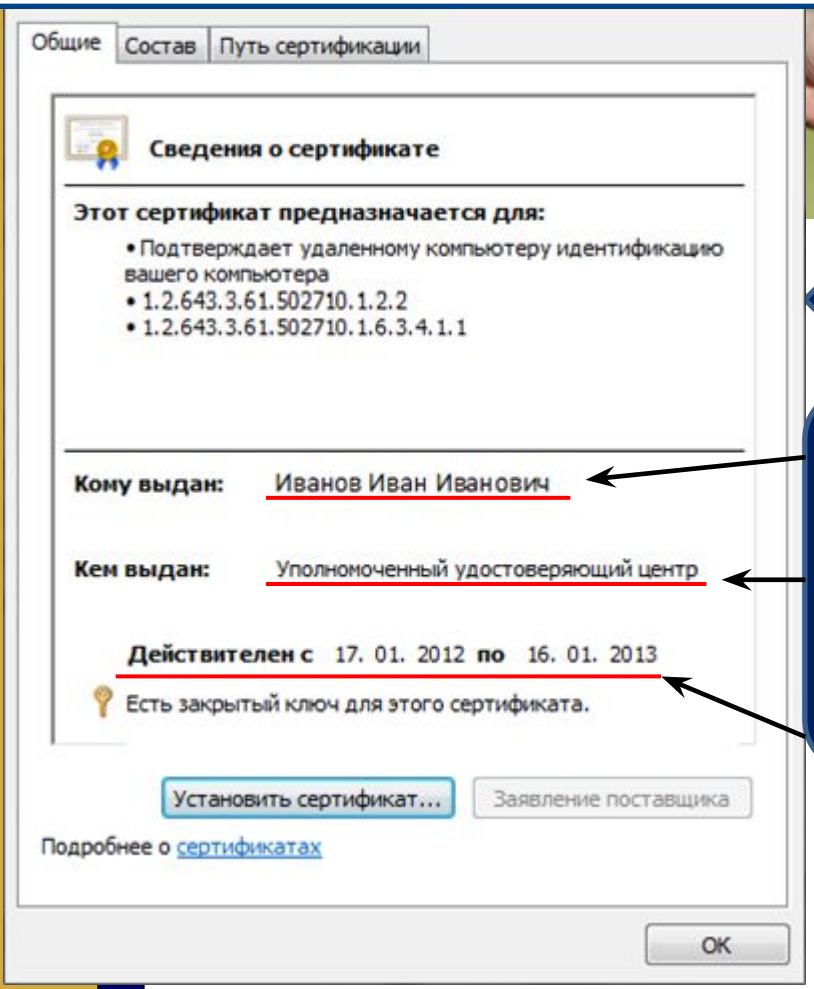
Усиленная подпись должна обязательно иметь сертификат аккредитованного Удостоверяющего центра

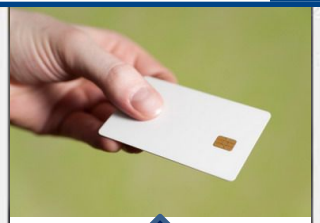
Список доверительных удостоверяющих центров

http://www.reestr-pki.ru/tsl.html

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Сертификат электронной подписи

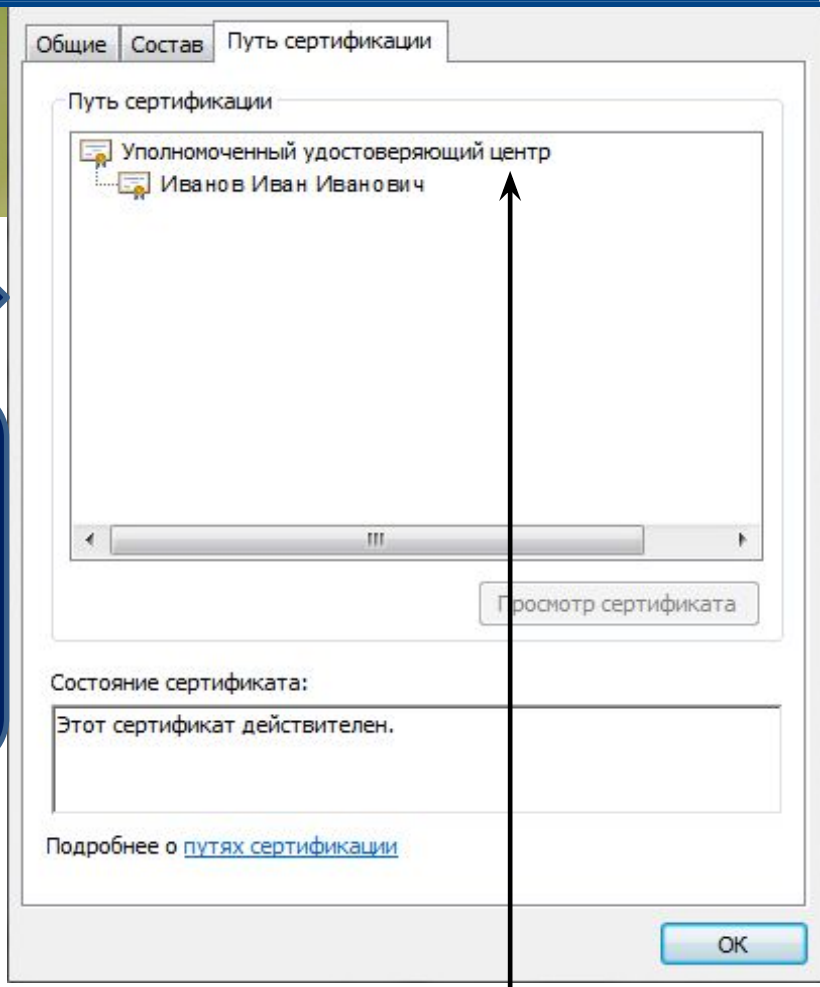




Ф.И.О

Кем выдан

Срок действия

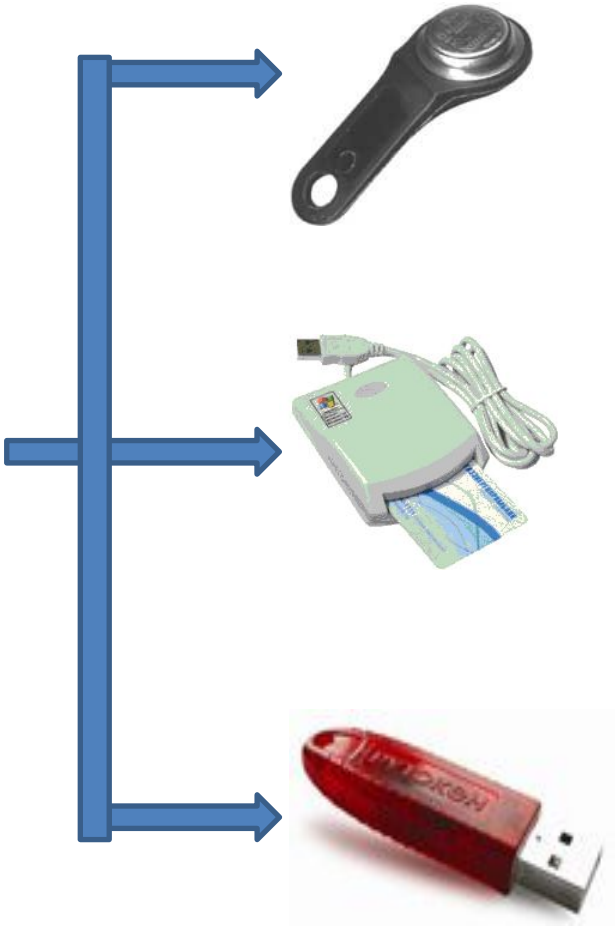


Сертификат удостоверяющего центра

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Носители ключевой информации (НКИ)

Типы носителя ключевой информации (усиленной квалифицированной электронной подписи)



АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

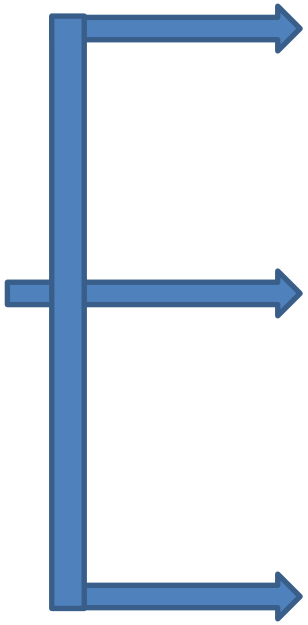
Носитель ключевой информации (НКИ)

Типы носителя ключевой информации (усиленной квалифицированной электронной подписи)

Криптопроцессорная смарт-карта для защищенного хранения и использования файлов, сертификатов, криптографических ключей

Программное обеспечение (ПО) для подписания документа

Типы ПО для подписания электронных документов



- Верба OW
- КриптоПро
- Криптон

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Программное обеспечение (ПО) для подписания документа

Типы ПО для подписания электронных документов

- Верба OW
- КриптоПро
- Криптон

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

ДОКУМЕНТЫ ФСБ России по криптозащите ПДн

Приказ ФСБ РФ от 27 декабря 2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи»

Приказ ФСБ России от 09.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. № 149/6/6-622, 2008 г., ФСБ России.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

ДОКУМЕНТЫ ФСБ России по криптозащите ПДн

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. № 149/54-144, 2008 г. ФСБ России.

Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных № 149/7/2/6-1173 08 августа 2009 г.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Средства электронной подписи

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2) позволяет определить лицо, подписавшее электронный документ;
3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
4) создается с использованием средств электронной подписи.
5) ключ проверки электронной подписи указан в квалифицированном сертификате;
6) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Порядок организации работ по использованию электронной подписи

1. Органам исполнительной власти Сахалинской области:

1.1. Определить должностное лицо органа исполнительной власти Сахалинской области ответственное за защиту информации и возложить на него полномочия, в том числе по получению, хранению и выдаче электронных подписей в установленном законом порядке. Подготовить «Журнал учета НКИ», «Журнал учета сертификатов», разработать инструкции пользователей ЭП.

1.2. Определить должностных лиц органа исполнительной власти Сахалинской области, ответственных за регистрацию межведомственных запросов и направление ответов на межведомственные запросы.

1.3. Произвести расчет по приобретению количества лицензий на программное обеспечение, а так же необходимого количества носителей ключевой информации.

1.4. В срок до 23 марта 2012 года представить данные о необходимом количестве лицензий на программное обеспечение и носителей ключевой информации в агентство по информационным технологиям и связи Сахалинской области.

2. Агентству по информационным технологиям и связи Сахалинской области в срок до 30 марта 2012 года:

2.1. Провести анализ потребности в количестве лицензий на программное обеспечение и носителей ключевой информации для органов исполнительной власти и органов местного самоуправления Сахалинской области.

2.2. Разработать регламент по закупке, установке и порядку эксплуатации ЭП.

АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ САХАЛИНСКОЙ ОБЛАСТИ

Спасибо за внимание!

ГБУ СО «Сахалинский областной центр информатизации»

693000, г. Южно-Сахалинск, Коммунистический проспект, 39, корпус «В», 4 этаж.
Тел: (4242) 49-88-97
e-mail: gbusocium@admsakhalin.ru
http://soci.admsakhalin.ru

По вопросам обращаться: Начальник отдела информационной безопасности Платонов Евгений Леонидович (4242) 49-79-88