Методические рекомендации по использованию электронной подписи при межведомственном электронном взаимодействии

Версия.4.3

Данные методические рекомендации разработаны в целях разъяснения наиболее часто встречающихся вопросов, связанных с формированием сертификатов и ключей электронной подписи (далее – ЭП) для использования при межведомственном электронном взаимодействии при предоставлении государственных услуг (исполнении государственных функций) с использованием Единой системы межведомственного электронного взаимодействия (далее – СМЭВ) и региональных систем межведомственного электронного взаимодействия (далее – РСМЭВ).

Методические рекомендации разработаны в целях реализации:

– Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

– Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее также – ФЗ № 63);

– Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (далее также – ФЗ № 1);

– Постановления Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия» (далее Постановление № 697);

– Постановления Правительства Российской Федерации от 8 июня 2011 г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;

– Постановления Правительства Российской Федерации от 28 ноября 2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи»;

– Распоряжения Правительства Российской Федерации от 12 июля 2011 № 1214-р об утверждении плана подготовки правовых актов в целях реализации федеральных законов «Об электронной подписи»;

– Приказа ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» (рег. Минюста России №23041 от 27.01.2012);

– Постановления Правительства Российской Федерации от 9 февраля 2012 года № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи»;

– Приказ Минкомсвязи России от 29.09.2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи в случае прекращения деятельности аккредитованного удостоверяющего центра» (рег. Минюста России № 22329 от 17.11.2011).;

– Приказ Минкомсвязи России от 05.10.2011 г. № 250 «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов а также предоставления информации из таких реестров» (рег. Минюста России № 22406 от 28.11.2011),

а также в рамках реализации:

– соглашений о взаимном признании электронных подписей, заключенных между Минкомсвязью России и органами государственной власти (федерального и регионального уровня, а также органами местного самоуправления) (далее – ОГВ, Методические рекомендации ЭП));

– соглашений о взаимодействии при обеспечении оказания (исполнения) государственных (муниципальных) услуг (функций) федеральными органами исполнительной власти, заключенных между Минкомсвязью России и органами исполнительной власти (далее – Методические рекомендации СМЭВ).

Данные методические рекомендации содержат:

Рекомендации по формированию и использованию сертификатов и ключей ЭП при межведомственном электронном взаимодействии при предоставлении государственных и муниципальных услуг (исполнении государственных и муниципальных функций), включая использование ЭП информационными системами ОГВ;

Рекомендации по выбору удостоверяющих центров (далее – УЦ) и требования к удостоверяющим центрам, которые осуществляют формирование и проверку сертификатов и ЭП.

Квалифицированный сертификат ключа проверки электронной подписи для межведомственного электронного взаимодействия

1. В рамках организации межведомственного электронного взаимодействия при предоставлении государственных и муниципальных услуг (исполнении государственных и муниципальных функций) применяется квалифицированный сертификат ключа проверки электронной подписи (далее – сертификат).

- Квалифицированный сертификат, используемый для формирования ЭП органа государственной власти (далее – ЭП-ОВ);
- Квалифицированный сертификат, используемый для формирования ЭП должностного лица ОГВ, уполномоченного направлять

межведомственные запросы и ответы на поступившие межведомственные запросы с использованием СМЭВ/РСМЭВ (далее – ЭП-СП).

2. Форма квалифицированного сертификата должна соответствовать приказу ФСБ России от 27 декабря 2011г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» (рег.№ 23041 от 27.01.2012).

3. В соответствии с положениями ФЗ № 63 квалифицированный сертификат выдается аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра**,** либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – УФО);
УФО в соответствии с Постановлением Правительства РФ № 976 «О Федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи» проводит аккредитацию и ведет перечень аккредитованных удостоверяющих центров.

*На переходный период до окончания действия ФЗ № 1 «Об электронной цифровой подписи» (до 30.06.2012г.) сертификаты, выданные доверенными удостоверяющими центрами Минкомсвязи России**,** входящими в единое пространство доверия, могут быть использованы для межведомственного электронного взаимодействия с использованием СМЭВ/РСМЭВ. После 01.07.2012 г. при межведомственном электронном взаимодействии будут использованы квалифицированные сертификаты. Сертификаты, выданные доверенными удостоверяющими центрами Минкомсвязи России до 01.07.2012, будут действительны до окончания срока их действия.*

4. Порядок формирования и проверки ЭП для СМЭВ регулируется актуальной версией “Методических рекомендаций по разработке электронных сервисов и применению технологии электронной подписи при межведомственном электронном взаимодействии” (далее – Методические рекомендации СМЭВ), размещенной на технологическом портале СМЭВ (smev.gosuslugi.ru).

5. Количество сертификатов ЭП-ОВ, выдаваемых для ОГВ (на юридическое лицо), рекомендуется ограничить количеством информационных систем ОГВ, используемых при межведомственном электронном взаимодействии, осуществляемом через СМЭВ/РСМЭВ;

Количество сертификатов ЭП-СП, выдаваемых для должностных лиц ОГВ, может быть ограничено количеством должностных лиц, уполномоченных для подписания электронных документов, направляемых с

использованием СМЭВ/РСМЭВ другим участникам информационного взаимодействия.

6. Правила заполнения полей сертификата будут определены документом «Рекомендации Минкомсвязи России по заполнению полей квалифицированного сертификата», подготавливаемым в настоящее время.
До публикации данных рекомендаций требования по заполнению полей сертификата изложены в данном документе.
Примеры сертификатов для ЭП-ОВ и ЭП-СП на переходный период до окончания действия ФЗ № 1 «Об электронной цифровой подписи» (до 30.06.2012г.) приведены в Приложении №2.

Обращается внимание:

При подготовке сведений для формирования сертификата ЭП-СП необходимо определить необходимость запроса сведений из Росреестра (выписки из ЕГРП).

- При необходимости такого запроса в поле “Улучшенный ключ” (OID=2.5.29.37) в сертификате ЭП-СП должен быть указан OID по требованиям Росреестра (Приложение № 1).

Примечание.

Указанные выше требования по внесению OID в сертификат действительны до ввода в эксплуатацию Единой системы идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме (Постановление Правительства Российской Федерации от 28 ноября 2011г. № 977) (далее – ЕСИА) в части регистра должностных лиц органов и организаций, и подключения к этому регистру поставщика сведений (Росреестра) и потребителей сведений (органов, предоставляющих государственные услуги с использованием информации, получаемой от Росреестра).

7. Ответственность за хранение и использование электронной подписи ЭП-ОВ и ЭП-СП обеспечивается организационно-техническими мероприятиями ОГВ.

Требования, предъявляемые к аккредитованным (доверенным) удостоверяющим центрам

8. Аккредитованный удостоверяющий центр должен удовлетворять требованиям аккредитации, иметь свидетельство об аккредитации, не находиться в списке удостоверяющих центров, у которых приостановлена или аннулирована аккредитация.

9. Удостоверяющие центры должны обеспечивать требования к качеству предоставления услуг:

– УЦ должны обеспечивать круглосуточный доступ к актуальным спискам отозванных сертификатов, размещенных в открытом доступе в информационно-телекоммуникационной сети «Интернет».

– Ссылка в информационно-телекоммуникационной сети «Интернет» на список отозванных сертификатов ЭП должна быть указана в сертификатах ЭП-ОВ и ЭП-СП.

– УЦ должны не позднее 1(одних) суток с момента выпуска нового корневого сертификата до начала его использования предоставить сертификат в электронном виде в Минкомсвязь России на адрес электронной почты ogs@minsvyaz.ru для использования в едином сервисе проверки Головного удостоверяющего центра (далее - универсальный сервис проверки).

– УЦ должны обеспечить возможность формирования сертификатов и ключей ЭП в соответствии с требованиями Федерального закона № 63 «Об электронной подписи», приказом ФСБ России «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» и данными Рекомендациями.

Требования, предъявляемые к участникам информационного взаимодействия для взаимодействия с использованием СМЭВ/РСМЭВ

10. Участник информационного взаимодействия с использованием СМЭВ (ОГВ, ИС которого непосредственно подключена к СМЭВ) должен заключить с Минкомсвязью России:

- соглашение о взаимодействии при обеспечении оказания (исполнения) государственных (муниципальных) услуг (функций);

Примечание.

При организации межуровневого взаимодействия («регион-федерация») передаваемое сообщение должно содержать в обязательном порядке как подпись ЭП-ОВ информационной системы регионального отправителя, так и подпись ЭП-РСМЭВ, формируемую региональным узлом СМЭВ. Также в электронном сообщении может содержаться ЭП-СП уполномоченного лица органа власти, от имени которого формируется ЭП-ОВ информационной системы регионального отправителя.

При обращении к федеральному узлу СМЭВ производится проверка ЭП-РСМЭВ, содержащейся в электронном сообщении. Именно на основании ЭП-РСМЭВ осуществляется разграничение доступа к сервисам федеральной СМЭВ, при этом на уровне СМЭВ не осуществляется проверка ЭП-ОВ регионального участника.

При обращении к региональному узлу СМЭВ со стороны регионального участника, происходит проверка ЭП-ОВ. Разграничение доступа к сервисам региональной СМЭВ (в том числе и к федеральным сервисам, зарегистрированным в региональном узле), осуществляется с использованием ЭП-ОВ регионального участника.

При этом необходимо отметить, что возможны ситуации, когда в субъекте РФ несколькими органами власти используется одна информационная система, имеющая, соответственно, один сертификат ЭП-ОВ. Но поскольку принадлежность сообщения конкретному органу власти субъекта РФ в данном случае для ЕСИА на уровне регистра информационных систем не очевидна (несколько органов власти пользуются данной ИС и, соответственно, её ЭП-ОВ), то разграничение доступа к сервисам региональной СМЭВ для отдельных органов власти субъекта РФ с использованием ЭП-ОВ невозможно, и его необходимо осуществлять оператору подобной информационной системы. Для возможности разграничения доступа на уровне РСМЭВ для информационных систем, используемых в субъекте РФ несколькими органами власти, необходимо обеспечить их доработку для обеспечения формирования различных ЭП-ОВ для каждого участника.

При организации межуровневого взаимодействия («федерация-регион») принципы формирования и проверки ЭП-СМЭВ и ЭП-ОВ являются аналогичными.

Структура сертификата ЭП-РСМЭВ должна соответствовать Приложению №3.

Структура сертификата ЭП-ОВ должна соответствовать Приложению №2 (Пример сертификата для ЭП-ОВ).

11. ОГВ должен:

– провести комплекс организационно-технических мероприятий, гарантирующих, что подписание ЭП-СП документа, отправляемого через СМЭВ/РСМЭВ, осуществляется только при наличии полномочий у должностного лица, сформировавшего документ и подписавшего его своей ЭП-СП в ИС ОГВ. *Данные мероприятия могут предусматривать использование ЕСИА после ввода данной системы в эксплуатацию и присоединения к ней участников информационного взаимодействия.*

– обеспечить возможность подписания сформированных электронных документов с применением сертифицированных средств электронной подписи и в соответствии с Методическими рекомендациями СМЭВ, как в автоматизированном, так и в автоматическом режимах.

– обеспечить возможность проверки ЭП и сертификатов ключей проверки для сформированных электронных документов в информационной системе ОГВ.

Требования к программно-аппаратным средствам, используемым для хранения ключевой информации

12. При выборе программно-аппаратных средств для хранения ключевой информации следует учитывать, что данное средство должно иметь сертификат ФСТЭК России, подтверждающий, что:

- данное устройство является программно-аппаратным средством аутентификации и хранения ключевой информации пользователей в автоматизированных системах до класса защищенности 1Г включительно;
- может использоваться при создании информационных систем персональных данных до 1 класса включительно.

При выборе в качестве программно-аппаратных средств для хранения ключевой информации устройств, реализующих криптографические алгоритмы и протоколы, указанные средства должны соответствовать требованиям приказа ФСБ России № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра» в соответствии с утвержденной для информационной системы ОГВ моделью угроз.

Рекомендуется использование ключевых носителей, соответствующих следующим требованиям:

- форм-фактор (по требованию информационных систем) - USB-ключ (предпочтительно) или смарт-карта;
- объем защищенной памяти не менее 32 КБ;
- поддерживаемые интерфейсы и стандарты - PKCS#11 версии v2.01 и выше (для носителей, являющихся СКЗИ, – не ниже v2.3), ISO 7816, Microsoft CryptoAPI, PC/CS (команды APDU), хранение сертификатов X.509 v3;
- ресурс EEPROM-памяти - не менее 500 000 циклов чтения/записи;
- срок хранения данных в памяти - не менее 10 лет;
- среднее время наработки на отказ электронных компонентов - не менее 10 лет;
- поддерживаемые операционные системы - Microsoft Windows семейства NT (32 и 64-битные версии), Linux;

Дополнительные комментарии

О проверке сертификатов и электронных подписей

13. Проверка сертификатов ключей проверки электронной подписи и корректности формирования электронной подписи может осуществляться сервисом проверки Информационной системы Головного удостоверяющего центра. Данный сервис зарегистрирован в СМЭВ (актуальный адрес размещения сервиса можно узнать с использованием технологического портала СМЭВ – smev.gosuslugi.ru), для обращения к нему на региональном уровне необходимо использовать адрес данного сервиса, зарегистрированного в соответствующем узле региональной СМЭВ.

Руководство пользователя электронного сервиса СМЭВ по «Сервису проверки электронной подписи подсистемы проверки и создания электронной подписи системы удостоверяющих центров единого пространства доверия электронного правительства» размещено на Технологическом портале СМЭВ (smev.gosuslugi.ru).

Необходимые шаги ОГВ и Минкомсвязи России

Выделенные курсивом положения настоящего раздела вступают в силу после ввода в эксплуатацию ЕСИА и подключения к ней участника информационного взаимодействия (ориентировочно, апрель 2012 года). Прочие положения необходимо применять незамедлительно.

14. ОГВ должны:

- определить уполномоченных лиц, наделенных в установленном ОГВ порядке полномочиями по использованию квалифицированной электронной подписи (ЭП-СП и ЭП-ОВ) в целях использования при межведомственном электронном взаимодействии. *После ввода в эксплуатацию ЕСИА и присоединения данного ОГВ к ЕСИА – обеспечить внесение в регистр должностных лиц ЕСИА сведений об указанных выше должностных лицах, используемых ими сертификатах ЭП-СП и их полномочиях по доступу к информационным ресурсам других участников информационного взаимодействия. Более детально данная процедура будет изложена в документах об использовании ЕСИА (Положение о ЕСИА, технический регламент подключения к ЕСИА и др.)*;
- организовать получение сертификатов ключей проверки электронной подписи ЭП-ОВ и ЭП-СП ОГВ в соответствии с п.3 ст.14 Федерального закона №63-ФЗ «Об электронной подписи» и данными Рекомендациями;
- провести организационно-технические мероприятия по организации технологической возможности подписания/проверки со стороны ОГВ электронных подписей уполномоченных лиц ОГВ и информационных систем ОГВ;
- представить сертификаты ЭП-ОВ и сведения об информационных системах ОГВ, которые используют данные сертификаты, в Минкомсвязь России для включения в регистр информационных систем ЕСИА. Более детально данная процедура изложена в Регламенте взаимодействия Участников информационного взаимодействия, Оператора единой системы межведомственного электронного взаимодействия и Оператора эксплуатации инфраструктуры электронного правительства при организации межведомственного взаимодействия с использованием единой системы межведомственного электронного взаимодействия (далее – Регламент, опубликован на Технологическом портале СМЭВ), *а также будет изложена*

в документах об использовании ЕСИА (Положение о ЕСИА, технический регламент подключения к ЕСИА).

– своевременно актуализировать в ЕСИА сведения о сертификатах ключей подписи ЭП-ОВ (для ЭП-ОВ возможно, путем направления в Минкомсвязь России формы сведений об ИС, в соответствии с Регламентом) *и ЭП-СП в соответствии с нормативными и методическими документами по использованию ЕСИА*.

– обеспечить процедуру подписи уполномоченными лицами исходящих из ИС ОГВ сообщений (электронных документов), а также обеспечить подписание ИС ОГВ исходящих в СМЭВ/РСМЭВ электронных документов с использованием сертификатов ЭП-ОВ в соответствии с актуальной версией Методических рекомендаций СМЭВ;

– обеспечить взаимное признание электронных подписей участников межведомственного электронного взаимодействия (далее – участники взаимодействия), для соблюдения условий, предусмотренных статьей 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» для электронных документов, поступающих в процессе информационного обмена участников взаимодействия посредством СМЭВ/РСМЭВ, в том числе путем использования универсального сервиса проверки головного удостоверяющего центра.

15. Для обеспечения возможности проверки сертификатов и электронных подписей участников взаимодействия Минкомсвязь России должна обеспечить круглосуточный доступ участникам информационного взаимодействия и к универсальному сервису проверки головного удостоверяющего центра.

Приложение 1.

Специфические идентификаторы Росреестра (применяются до ввода в эксплуатацию ЕСИА – см. п. 6)

№ п/п	Номер идентификатора	Значение идентификатора	Расшифровка
1	1.2.643.5.1.24.2.20	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель федерального органа исполнительной власти или иное уполномоченное лицо данного органа в соответствии с федеральным законом
2	1.2.643.5.1.24.2.43	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель территориального органа федерального органа исполнительной власти или иное уполномоченное лицо данного органа в соответствии с федеральным законом
3	1.2.643.5.1.24.2.6	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель органа государственной власти субъекта Российской Федерации или иное уполномоченное лицо данного органа в соответствии с федеральным законом
4	1.2.643.5.1.24.2.19	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель органа местного самоуправления или иное уполномоченное лицо данного органа в соответствии с федеральным законом

Приложение 2

Пример сертификата для ЭП-СП

(Рекомендован до утверждения Рекомендаций по применению приказа Приказа ФСБ России от 27 декабря 2011г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» (рег. Минюста России №23041 от 27.01.2012»)

Сведения о сертификате:
Кому выдан:
Иванов Иван Иванович
Кем выдан:
УЦ ОГИЦ ВУ_1
Действителен с 28 октября 2011 г. 12:16:00 UTC по 28 октября 2012 г. 12:17:00 UTC
Версия: 3 (0x2)
Серийный номер: 52C3 C43C 0000 0000 0E54
Издатель сертификата: CN = УЦ ОГИЦ ВУ_1, OU = УГУ, O = ООО, L = Москва, C = RU, E = uc2_1@nii.aaa.ru
Срок действия:
Действителен с: 28 октября 2011 г. 12:16:00 UTC
Действителен по: 28 октября 2012 г. 12:17:00 UTC
Владелец сертификата: T = Заместитель директора ФФФ России, CN = Иванов Иван Иванович, O = Федеральная служба, C = RU, E = exp2@faaa.ru
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 2445 D53E 7837 EC34 DED3 CCBA EF9E FEFB 8D2F 0BC4 E500 E1F9 0B27 94CE 42C4 373F 9F4E B038 93C5 E34F B2A7 27EC 797A AB2C 225D 426E 15C9 3682 5318 A675 CCFA B81A
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 1.2.840.113549.1.9.15
Название: Возможности SMIME
Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
3. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Руководитель ФОИВ или иное уполномоченное лицо данного органа в соответствии с федеральным законом (1.2.643.5.1.24.2.20)
4. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта
Значение: 91 a2 b4 25 20 6d e1 df 91 3d cf 0b 15 6e 0b e5 c1 9b 78 c8
5. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=65 57 77 60 e1 5b ea 59 00 7a 32 6f 16 f5 4e 0d 05 0b 25 29
6. Расширение 2.5.29.32
Название: Политики применения
Значение: [1]Политика сертификата приложения: [2]Политика сертификата приложения: Идентификатор политики=Пользователь Центра Регистрации, HTTP, TLS клиент [3]Политика сертификата приложения: Идентификатор политики=Проверка подлинности клиента
7. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://uc.ogic.ru/CDP/UC_OGIC_VU_1.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cdp1.ogic.ru/CDP/UC_OGIC_VU_1.crl
8. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://uc.ogic.ru/CERTS/UC_OGIC_VU_1.cer
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: 9F0C 9D30 46C0 C2F5 B7BF 73C0 C3A9 CFD5 E43A 5187 5413 5C25 53B8 1D9D A102 E73F 1F5E 64DE 4269 DD31 DF91 D5E1 BE3E 51E1 157E 4586 2DA7 C240 A94A 0191 C207 4A2C
Средство ЭЦП:
Крипто Про CSP 3.0

Пример сертификата для ЭП-ОВ

(Рекомендован до утверждения Рекомендаций по применению приказа Приказа ФСБ России от 27 декабря 2011г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» (рег. Минюста России №23041 от 27.01.2012»)

Сведения о сертификате:
Кому выдан:
Служба ФФ
Кем выдан:
УЦ ОГИЦ ВУ_1
Действителен с 28 октября 2011 г. 11:15:00 UTC по 28 октября 2012 г. 11:16:00 UTC
Версия: 3 (0x2)

Серийный номер: 528C 1DA7 0000 0000 0E52
Издатель сертификата: CN = УЦ ОГИЦ ВУ_1, OU = УГУ, O =ООО, L = Москва, C = RU, E = uc2_1@nii.faa.ru
Срок действия:
Действителен с: 28 октября 2011 г. 11:15:00 UTC
Действителен по: 28 октября 2012 г. 11:16:00 UTC
Владелец сертификата: CN = Служба ФФ, O = Федеральная служба , C = RU
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 7A69 891F F348 79EE B493 15CD 9235 00AB F6F5 C5E2 B7BF 1ED1 3E36 EF22 59C7 2C0A 6451 539D 141B 1358 91DC 659B E9EB 312D C2D8 2266 1F31 1D39 0CD4 DE15 17E1 868D
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 1.2.840.113549.1.9.15
Название: Возможности SMIME
Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
3. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
4. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 6b 3b 01 e6 82 d8 60 be 9a da 21 71 82 50 a8 e0 9a e1 fd ea
5. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=65 57 77 60 e1 5b ea 59 00 7a 32 6f 16 f5 4e 0d 05 0b 25 29
6. Расширение 2.5.29.32
Название: Политики применения
Значение: [1]Политика сертификата приложения: [2]Политика сертификата приложения: Идентификатор политики=Пользователь Центра Регистрации, HTTP, TLS клиент [3]Политика сертификата приложения: Идентификатор политики=Проверка подлинности клиента
7. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://uc.ogic.ru/CDP/UC_OGIC_VU_1.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cdp1.ogic.ru/CDP/UC_OGIC_VU_1.crl
8. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://uc.ogic.ru/CERTS/UC_OGIC_VU_1.cer
Подпись Удостоверяющего центра:

Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: AB6F 4170 0B3A F174 E1EA 2654 9470 E9F1 004E 10BA DCC9 6C42 0974 05AC 2CC0 1C80 5899 955F B5CD A96B 203E DF28 ACBF BB06 B125 8E84 097A 75CB AC9B 4D85 0F77 A522
Средство ЭЦП:
Крипто Про CSP 3.0

Приложение №3

Пример сертификата для информационной системы

(Рекомендован до утверждения Рекомендаций по применению приказа Приказа ФСБ России от 27 декабря 2011г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» (рег. Минюста России №23041 от 27.01.2012»)

Сведения о сертификате:
Кому выдан:
Информационная система
Кем выдан:
УЦ ОГИЦ ВУ_1
Действителен с 28 октября 2011 г. 11:15:00 UTC по 28 октября 2012 г. 11:16:00 UTC
Версия: 3 (0x2)
Серийный номер: 528C 1DA7 0000 0000 0E52
Издатель сертификата: CN = УЦ ОГИЦ ВУ_1, OU = УГУ, O =ООО, L = Москва, C = RU, E = uc2_1@nii.faa.ru
Срок действия:
Действителен с: 28 октября 2011 г. 11:15:00 UTC
Действителен по: 28 октября 2012 г. 11:16:00 UTC
Владелец сертификата: CN = Информационная система, O = Федеральная служба , C = RU
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 7A69 891F F348 79EE B493 15CD 9235 00AB F6F5 C5E2 B7BF 1ED1 3E36 EF22 59C7 2C0A 6451 539D 141B 1358 91DC 659B E9EB 312D C2D8 2266 1F31 1D39 0CD4 DE15 17E1 868D
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 1.2.840.113549.1.9.15
Название: Возможности SMIME

Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
3. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
4. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 6b 3b 01 e6 82 d8 60 be 9a da 21 71 82 50 a8 e0 9a e1 fd ea
5. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=65 57 77 60 e1 5b ea 59 00 7a 32 6f 16 f5 4e 0d 05 0b 25 29
6. Расширение 2.5.29.32
Название: Политики применения
Значение: [1]Политика сертификата приложения: [2]Политика сертификата приложения: Идентификатор политики=Пользователь Центра Регистрации, HTTP, TLS клиент
[3]Политика сертификата приложения: Идентификатор политики=Проверка подлинности клиента
7. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://uc.ogic.ru/CDP/UC_OGIC_VU_1.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cdp1.ogic.ru/CDP/UC_OGIC_VU_1.crl
8. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://uc.ogic.ru/CERTS/UC_OGIC_VU_1.cer

Подпись Удостоверяющего центра:

Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: AB6F 4170 0B3A F174 E1EA 2654 9470 E9F1 004E 10BA DCC9 6C42 0974 05AC 2CC0 1C80 5899 955F B5CD A96B 203E DF28 ACBF BB06 B125 8E84 097A 75CB AC9B 4D85 0F77 A522

Средство ЭЦП:

Крипто Про CSP 3.0