Методические рекомендации по использованию электронной подписи при предоставлении информации в ГИС ТЭК

## Нормативная база

Методические рекомендации разработаны на основании:

* 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»;
* Приказа 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).;
* Приказа 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).

## Термины и определения

Таблица — Термины и определения

| Сокращение | Аналог в СМЭВ | Термин  |
| --- | --- | --- |
| УЦ |  | Удостоверяющий центр |
| ЭП | ЭП | Сертификаты и ключи электронной подписи |
| ЭП-Субъекта, Технологическая подпись,  | ЭП-ОВ | Квалифицированный сертификат, используемый для формирования ЭП Субъекта ГИС ТЭК, в том числе органа государственной власти, юридического лица и т.д. |
| ЭП-УЛ | ЭП-СП | ЭП уполномоченного лица Субъекта ГИС ТЭК |
| Методические рекомендации ЭП |  | Методические рекомендации по использованию электронной подписи при межведомственном электронном взаимодействии. Версия 4.3 |
| Сертификат |  | квалифицированный сертификат ключа проверки электронной подписи |
| ФЗ № 63 |  | Федеральный закон от 06.04.2011 N 63-ФЗ«Об электронной подписи» |
| УФО |  | Уполномоченный федеральный орган. Федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи |
| СМЭВ | СМЭВ | Системе межведомственного электронного взаимодействия |

## Сертификат ключа проверки ЭП

В рамках организации информационного взаимодействия с ГИС ТЭК применяются следующие квалифицированные сертификаты:

* Квалифицированный сертификат, используемый для формирования ЭП информационной системы Субъекта ГИС ТЭК (ЭП-Субъекта). ЭП-Субъекта в случае органов государственной власти соответствует ЭП-ОВ СМЭВ, для иных юридических лиц – ЭП, выданная юридическому лицу;
* Квалифицированный сертификат, используемый для формирования ЭП уполномоченного лица Субъекта ГИС ТЭК (ЭП-УЛ). ЭП-УЛ для органов государственной власти соответствует ЭП-СП СМЭВ, для иных юридических лиц – ЭП, выданная уполномоченному лицу юридического лица, либо физическому лицу.

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).

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.

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.

В настоящее время, УФО является Министерство связи и массовых коммуникаций Российской Федерации.

Порядок формирования и проверки ЭП для организации информационного взаимодействия с ГИС ТЭК аналогичен требованиям СМЭВ, описанным в «Методических рекомендациях 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).

Количество сертификатов ЭП-Субъекта, выдаваемых для на юридическое лиц, рекомендуется ограничить количеством информационных систем Субъекта ГИС ТЭК, используемых при взаимодействии с ГИС ТЭК.

Количество сертификатов ЭП-УЛ, выдаваемых для уполномоченных лиц Субъекта ГИС ТЭК, может быть ограничено количеством представителей Субъекта ГИС ТЭК, уполномоченных для подписания электронных документов, направляемых в ГИС ТЭК.

Правила заполнения полей сертификата должны быть определены Минкомсвязи России. До публикации данных, соответствующего нормативного акта требования по заполнению полей сертификата изложены в Методических рекомендациях ЭП..

Ответственность за хранение и использование электронной подписи ЭП-Субъекта и ЭП-УЛ обеспечивается организационно-техническими мероприятиями Субъекта ГИС ТЭК.

## Требования к УЦ

Удостоверяющие центры должны советовать требованиям Минкомсвязи России, изложенным в Методических рекомендациях ЭП.

## Требования к участникам информационного взаимодействия

Участник информационного взаимодействия должен:

* заключить Оператором ГИС ТЭК соглашение о взаимодействии при предоставлении информации в ГИС ТЭК;
* определить уполномоченных лиц, наделенных в установленном Субъектом ГИС ТЭК порядке полномочиями по использованию квалифицированной электронной подписи (ЭП-УЛ и ЭП-Субъекта) в целях использования при предоставлении информации в ГИС ТЭК;
* организовать получение сертификатов ключей проверки электронной подписи ЭП-Субъекта и ЭП-УЛ 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 Субъекта ГИС ТЭК электронных подписей уполномоченных лиц Субъекта ГИС ТЭК и информационных систем Субъекта ГИС ТЭК;
* представить сертификаты ЭП-Субъекта, ЭП-УЛ и сведения об информационных системах Субъекта ГИС ТЭК, которые используют данные сертификаты, в Оператору ГИС ТЭК для регистрации информационной системы в ГИС ТЭК;
* своевременно актуализировать в ГИС ТЭК сведения о сертификатах ключей подписи ЭП-Субъекта и ЭП-УЛ;
* обеспечить взаимное признание электронных подписей участников информационного взаимодействия.

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

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 Субъекта ГИС ТЭК 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.