**Приложение № 10 к Регламенту**

Общая структура квалифицированного сертификата ключа

проверки электронной подписи

|  |  |  |
| --- | --- | --- |
| **Название** | **Описание** | **Содержание** |
| **Базовые поля сертификата** | | |
| Version | Версия | V3 |
| Serial Number | Серийный номер | Уникальный серийный номер сертификата |
| Signature Algorithm | Алгоритм подписи | ГОСТ Р 34.11/34.10-2001 |
| Issuer | Издатель сертификата | Атрибуты имени Удостоверяющего центра |
| Validity Period | Срок действия сертификата | Действителен с: дд.мм.гггг чч:мм:сс GMT  Действителен по: дд.мм.гггг чч:мм:сс GMT |
| Subject | Владелец сертификата | Атрибуты имени Владельца сертификата |
| Public Key | Открытый ключ | Открытый ключ (алгоритм ГОСТ Р 34.10-2001) |
| Issuer Signature Algorithm | Алгоритм подписи издателя сертификата | ГОСТ Р 34.11/34.10-2001 |
| Issuer Sign | ЭЦП издателя сертификата | Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 |
| **Дополнения сертификата** | | |
| Key Usage (critical) | Использование ключа | Проверка ЭП под ЭД (кроме сертификатов и списков отозванных сертификатов); невозможность отказа от ЭП под ЭД (кроме сертификатов и списков отозванных сертификатов); зашифрование закрытых и секретных ключей; зашифрование данных; согласование ключей |
| Subject Key Idendifier | Идентификатор ключа владельца сертификата | Идентификатор закрытого ключа владельца сертификата |
| Authority Key Identifier | Идентификатор ключа издателя сертификата | Идентификатор закрытого ключа Удостоверяющего центра, которым подписан данный сертификат |
| Certificate Policies | Политики сертификации | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |
| CRL Distribution Points | Точки распространения списка отозванных сертификатов (CRL) | Адреса, по которым Удостоверяющий центр публикует Списки отозванных сертификатов |
| Authority Information Access | Точки распространения сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра | Адреса, по которым Удостоверяющий центр опубликовал Сертификат Удостоверяющего центра, атрибуты имени которого указаны в поле «Издатель сертификата» |
| SubjectSignTool | Наименование средства ЭП, используемое владельцем сертификата | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |
| IssuerSignTool | Наименование средств ЭП и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, а также реквизиты документов, подтверждающих соответствие указанных средств требованиям, установленным 63-ФЗ | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |