Приложение № 4

к Техническим нормам

в области электронной подписи

**Структура сертификата открытого ключа службы метки времени (TSP), службы on-line проверки статуса сертификата (OCSP) и службы подтверждения достоверности данных и протокол сервера сертификации (DVCS)**

Сертификат открытого ключа служб TSP, OCSP или DVCS содержит следующие поля:

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование (на англ. языке)** | **Описание** | **Содержание** | **ПРИМЕЧАНИЕ** |
| ***Базовые поля*** | | | |
| Version | Версия | V3 |  |
| Serial Number | Регистрационный номер сертификата | Номер |  |
| Issuer | Идентификационные данные поставщика сертификационных услуг, издателя  сертификата | CN = Наименование поставщика сертификационных услуг  L = Населенный пункт  S = Государство  OU = Поставщик сертификационных услуг, подразделение юридического лица  O = Наименование юридического лица, IDNO  C = Код государства |  |
| Validity | Срок действия сертификата | Действителен с: «\_\_» \_\_\_\_\_\_ 20\_\_ г. чч:мм:сс GMT  Действителен по: «\_\_» \_\_\_\_\_ 20\_\_ г. чч:мм:сс GMT |  |
| Subject | Идентификационные данные поставщика сертификационных услуг | CN = Наименование поставщика сертификационных услуг  L = Населенный пункт  S = Государство  OU = Поставщик сертификационных услуг, подразделение юридического лица  O = Наименование юридического лица, IDNO  C = Код государства |  |
| Subject Public Key Info | Открытый ключ | Открытый ключ поставщика сертификационных услуг |  |
| Signature Algorithm | Алгоритм подписи издателя сертификата | Наименование алгоритма электронной подписи издателя сертификата |  |
| Signature Value | Электронная подпись издателя сертификата | Подпись издателя в соответствии с используемым алгоритмом |  |
| ***Дополнительные поля*** | | | |
| Authority Key Identifier | Идентификатор ключа издателя сертификата | Идентификатор закрытого ключа поставщика сертификационных услуг, выпустившего данный сертификат |  |
| Subject Key Identifier | Идентификатор ключа владельца сертификата | Идентификатор закрытого ключа поставщика сертификационных услуг, соответствующего данному сертификату |  |
| Key Usage | Использование ключа | Неотрекаемость, электронная подпись | НЕКРИТИЧНО |
| Certificate Policies | Политика сертификации поставщика сертификационных услуг | Идентификатор политики = все политики выдачи.  Сведения квалификатора политики | Может быть  КРИТИЧНО |
| Basic Constraints | Основные ограничения | Тип субъекта = конечный пользователь  Ограничение на длину пути = отсутствует | Может присутствовать  и может быть  КРИТИЧНО |
| CRL Distribution Point | Точка распределения списка отозванных сертификатов | Источник опубликования списка отозванных сертификатов |  |
| Extended Key Usage | Расширенная область применения ключа | Идентификатор, определяющий, что сертификат предназначен для службы метки времени (TSP), для службы on-line проверки статуса сертификата (OCSP) или для службы подтверждения достоверности данных и протокола сервера сертификации (DVCS) | КРИТИЧНО |
| Authority Information Access | Доступ к сведениям поставщика сертификационных услуг | Метод доступа к информации поставщика сертификационных услуг |  |