Приложение № 5

к Регламенту Поставщика сертификационных услуг

в области применения усиленной квалифицированной

электронной подписи

**Структура сертификата открытого ключа**

**Поставщика сертификационных услуг второго уровня**

Сертификат открытого ключа Поставщика сертификационных услуг второго уровня содержит следующие поля:

|  |  |  |
| --- | --- | --- |
| **Наименование**  **(на англ. языке)** | **Описание** | **Содержание** |
| ***Базовые поля*** | | |
| Version | Версия | V3 |
| Serial Number | Регистрационный номер сертификата | Номер |
| Issuer | Идентификационные данные Поставщика высшего уровня | CN = Наименование поставщика  L = Кишинэу  S = Республика Молдова  OU = Поставщик высшего уровня  O = SIS RM, IDNO  C = MD |
| Validity | Срок действия  сертификата | Действителен с: "\_\_" \_\_\_\_\_ 20\_\_ г. чч:мм:сс GMT  Действителен по: "\_\_" \_\_\_\_ 20\_\_ г. чч:мм:сс GMT |
| Subject | Идентификационные данные Поставщика второго уровня | 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 |
| Signature  Algorithm | Алгоритм подписи  издателя  сертификата | SHA-1/RSA |
| Signature Value | Электронная подпись издателя сертификата | Подпись издателя в соответствии с SHA-1/RSA |
| ***Дополнительные поля*** | | |
| Autority Key  Identifier | Идентификатор ключа эмитента сертификата | Идентификатор закрытого ключа поставщика сертификации высшего уровня |
| Subject Key  Identifier | Идентификатор ключа владельца сертификата | Идентификатор закрытого ключа поставщика сертификации высшего уровня |
| Key Usage | Использование ключа | Электронная подпись в сертификатах, электронная подпись в списке отозванных сертификатов |
| Private Key Usage Period | Период действия закрытого ключа | Действителен с: "\_\_" \_\_\_\_\_ 20\_\_ г. чч:мм:сс GMT  Действителен по: "\_\_" \_\_\_\_ 20\_\_ г. чч:мм:сс GMT |
| Certificate Policies | Политика сертификации поставщика сертификационных услуг | Идентификатор политики = все политики выдачи.  Сведения квалификатора политики |
| Basic Constraints | Основные ограничения | Тип субъекта = СА  Ограничение на длину пути = отсутствует = 1 |
| CRL Distribution Point | Точка распределения списка отозванных сертификатов (CRL) | URL= http://www.pki.sis.md/ххх |
| Authority Information Access | Доступ к сведениям поставщика сертификационных услуг | Метод доступа к информации о поставщике сертификационных услуг |