Приложение № 1

к Регламенту Поставщика сертификационных услуг

в области применения усиленной квалифицированной

электронной подписи

**Структура сертификата открытого ключа**

**Поставщика сертификационных услуг высшего уровня**

Сертификат открытого ключа Поставщика сертификационных услуг высшего 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 высшего уровня | CN = Наименование поставщика  L = Кишинэу  S = Республика Молдова  OU = Поставщик высшего уровня  O = SIS RM, IDNO  C = MD |
| Subject Public Key Info | Открытый ключ | Открытый ключ (RSA) |
| 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*** | | |
| Subject Key  Identifier | Идентификатор ключа владельца сертификата | Идентификатор закрытого ключа Поставщик высшего уровня, соответствующего данному сертификату |
| Key Usage | Использование ключа | Электронная подпись в сертификатах, электронная подпись в списке отозванных сертификатов (CRL) |
| 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 |
| CRL Distribution  Point | Точка распределения списка отозванных сертификатов (CRL) | URL= http://www.pki.sis.md/ххх |