Утвержден
приказом Федеральной службы
по регулированию алкогольного рынка
от _____ № ____

Порядок
представления в электронном виде деклараций
об объемах производства, оборота и (или) использования
этилового спирта, алкогольной и спиртосодержащей продукции,
об использовании производственных мFощностей

I. Общие положения

Декларации об объемах производства, закупки (в том числе импорта), поставки (в том числе экспорта), хранения, перевозки и (или) использования этилового спирта, алкогольной и спиртосодержащей продукции, об использовании производственных мощностей (далее – декларации) представляются организациями, осуществляющими производство, оборот и (или) использование этилового спирта, алкогольной и спиртосодержащей продукции в Росалкогольрегулирование в электронном виде, в установленном формате, посредством передачи по телекоммуникационным каналам связи с электронной подписью, соответствующей требованиям Приложения 1 к данному приказу.

2. Декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции представляются организациями, осуществляющими розничную продажу алкогольной и спиртосодержащей продукции, и индивидуальными предпринимателями, осуществляющими розничную продажу пива и пивных напитков в органы государственной власти субъектов Российской Федерации в области производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции (далее – органы власти субъектов РФ) каждого субъекта Российской Федерации, на территории которых указанные организации, на основании соответствующей лицензии, или индивидуальный предприниматель осуществляют деятельность по розничной продаже алкогольной (в том числе пива и пивных напитков) и

спиртосодержащей продукции в электронном виде, в установленном формате, посредством передачи по телекоммуникационным каналам связи с электронной подписью, соответствующей требованиям Приложения 1 к данному приказу. Перечень удостоверяющих центров определяется органами власти субъектов РФ с согласования Росалкогольрегулирования.

3. Копии деклараций об объемах розничной продажи алкогольной и спиртосодержащей продукции, представленные в соответствии с пунктом 2 настоящего Порядка, представляются организациями, осуществляющими розничную продажу алкогольной и спиртосодержащей продукции и индивидуальными предпринимателями, осуществляющими розничную продажу пива и пивных напитков в Росалкогольрегулирование в электронном виде, в установленном формате, посредством передачи по телекоммуникационным каналам связи с электронной подписью.

Организации, осуществляющие розничную продажу алкогольной и спиртосодержащей продукции, и индивидуальные предприниматели, осуществляющие розничную продажу пива и пивных напитков, представляют в Росалкогольрегулирование копию декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции, полученную в соответствии с подпунктом "в" пункта 8.2 настоящего Порядка, от органа власти субъекта РФ, на территории которого зарегистрировано место нахождение (юридический адрес) юридического лица или место государственной регистрации индивидуального предпринимателя.

4. Отношения между участниками информационного обмена при представлении деклараций по телекоммуникационным каналам связи регулируются Федеральным законом от 22 ноября 1995 г. № 171-ФЗ "О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции" (Собрание законодательства Российской Федерации, 1995, № 48, ст. 4553; 1999, № 2, ст. 245; 2001, № 53, ст. 5022; 2002, № 30, ст. 3026, 3033; 2004, № 45, ст. 4377; 2005, № 30, ст. 3113; 2006, № 31,

ст. 3433, № 43, ст. 4412; 2007, № 1, ст. 11, № 17, ст. 1931, № 31, ст. 3994, № 49, ст. 6063; 2008, № 30, ст. 3616; 2009, № 1, ст. 21, № 52, ст. 6450; 2010, № 15, ст. 1737, № 31, ст. 4196; 2011, № 1, ст. 42, № 27, ст. 3880, № 30, ст. 4566, ст. 4601), Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036, № 37, ст. 3880), Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, 4196; 2011, № 15, ст. 2038), постановлением Правительства Российской Федерации от ___ _____ 2012 г. № ___ "О представления деклараций об объемах производства, оборота и (или) использования этилового спирта, алкогольной и спиртосодержащей продукции, об использовании производственных мощностей" (Собрание законодательства Российской Федерации, 2012, №___, ст. ____), приказом Росалкогольрегулирования от 15 марта 2010 г. № 24н "Об утверждении порядка заполнения деклараций об объемах производства, оборота и использования этилового спирта, алкогольной и спиртосодержащей продукции" (Зарегистрирован в Министерстве юстиции Российской Федерации 23 августа 2010 г. № 18222) и другими нормативными правовыми актами, а также настоящим Порядком.

II. Порядок представления деклараций об объемах производства, закупки (в том числе импорта), поставки (в том числе экспорта), хранения, перевозки и (или) использования этилового спирта, алкогольной и спиртосодержащей продукции, об использовании производственных мощностей

5. При представлении организацией, осуществляющей производство, оборот и (или) использование этилового спирта, алкогольной и спиртосодержащей продукции декларации по телекоммуникационным каналам связи соблюдается следующий порядок электронного документооборота:

5.1. Каждая подготовленная в соответствии с утвержденным Росалкогольрегулированием форматом декларация подписывается электронной

подписью руководителя организации (руководителя филиала организации, уполномоченного заместителя руководителя организации), осуществляющей производство, оборот и (или) использование этилового спирта, алкогольной и спиртосодержащей продукции, и направляется в зашифрованном виде по телекоммуникационным каналам связи в информационную систему Росалкогольрегулирования.

5.2. В течение суток с момента отправки декларации организация, осуществляющая производство, оборот и (или) использование этилового спирта, алкогольной и спиртосодержащей продукции получает от Росалкогольрегулирования:

а) протокол форматно-логического контроля декларации. В случае наличия в протоколе форматно-логического контроля декларации ошибок, организация, осуществляющая производство и оборот этилового спирта, алкогольной и спиртосодержащей продукции, принимает меры по их устранению и повторяет всю процедуру представления декларации.

б) квитанцию о приеме декларации по телекоммуникационным каналам связи. Указанную квитанцию организация, осуществляющая производство и оборот этилового спирта, алкогольной и спиртосодержащей продукции, получает в случае успешного прохождения декларацией форматно-логического контроля.

6. Если организация, осуществляющая производство, оборот и (или) использование этилового спирта, алкогольной и спиртосодержащей продукции, не получила от Росалкогольрегулирования в установленное время квитанцию о приеме декларации по телекоммуникационным каналам связи и (или) протокол форматно-логического контроля декларации, она информирует Росалкогольрегулирование о данном факте с использованием информационных ресурсов Росалкогольрегулирования.

7. Датой представления деклараций по телекоммуникационным каналам связи является дата ее получении, указанная в квитанции о приеме декларации по телекоммуникационным каналам связи.

III. Порядок представления деклараций об объемах розничной продажи алкогольной и спиртосодержащей продукции

8. При представлении организацией, осуществляющей розничную продажу алкогольной и спиртосодержащей продукции, и индивидуальным предпринимателем, осуществляющим розничную продажу пива и пивных напитков (далее – индивидуальный предприниматель), декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции по телекоммуникационным каналам связи соблюдается следующий порядок электронного документооборота:

8.1. Каждая подготовленная в соответствии с утвержденным Росалкогольрегулированием форматом декларация об объемах розничной продажи алкогольной и спиртосодержащей продукции подписывается электронной подписью индивидуального предпринимателя или руководителя организации (руководителя филиала организации, уполномоченного заместителя руководителя организации), осуществляющей розничную продажу алкогольной и спиртосодержащей продукции, и направляется в зашифрованном виде по телекоммуникационным каналам связи в информационную систему органа власти субъекта РФ, на территории которого указанная организация, на основании соответствующей лицензии, или индивидуальный предприниматель осуществляют деятельность по розничной продаже алкогольной (в том числе пива и пивных напитков) и спиртосодержащей продукции.

Шифрование представляемой декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции выполняется организацией, осуществляющей розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальным предпринимателем с использованием ключей шифрования, принадлежащих Росалкогольрегулированию и органу власти субъекта РФ, в адрес которого направляется указанная декларация.

8.2. В течение суток с момента отправки декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель получает от органа власти субъекта РФ:

а) протокол форматно-логического контроля декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции. В случае наличия в указанном протоколе ошибок, организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель принимает меры по их устранению и повторяет всю процедуру представления декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции;

б) квитанцию о приеме декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции по телекоммуникационным каналам связи. Указанную квитанцию организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель получает в случае успешного прохождения декларацией об объемах розничной продажи алкогольной и спиртосодержащей продукции форматно-логического контроля;

в) копию представленной декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции, подписанную электронной подписью органа власти субъекта РФ, принявшего данную декларацию.

9. Если организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель не получат от органа власти субъекта РФ в установленное время квитанцию о приеме по телекоммуникационным каналам связи декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции или протокол форматно-логического контроля такой декларации, указанная организация или индивидуальный предприниматель информируют орган власти субъекта РФ о данном факте письменно или с использованием информационных ресурсов органа власти субъекта РФ.

10. Датой представления декларации об объемах розничной продажи алкогольной продукции по телекоммуникационным каналам связи является дата ее получении, указанная в квитанции о приеме указанной декларации по телекоммуникационным каналам связи.

IV. Порядок представления копий деклараций об объемах розничной продажи алкогольной и спиртосодержащей продукции

11. После получения организацией, осуществляющей розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальным предпринимателем от органа власти субъекта РФ копии декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции, указанной в подпункте "в" пункта 8.2 настоящего Порядка, данная организация или индивидуальный предприниматель направляет ее в электронном виде, по телекоммуникационным каналам связи в информационную систему Росалкогольрегулирования.

12. В течение суток с момента отправки копии декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель получает от Росалкогольрегулирования:

а) протокол форматно-логического контроля копии декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции. В случае наличия в указанном протоколе ошибок, организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель принимает меры по их устранению и повторяет всю процедуру представления копии декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции.

б) квитанцию о приеме копии декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции по телекоммуникационным

каналам связи. Указанную квитанцию организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель получает в случае успешного прохождения копией декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции форматно-логического контроля.

13. Если организация, осуществляющая розничную продажу алкогольной и спиртосодержащей продукции, или индивидуальный предприниматель не получат от Росалкогольрегулирования в установленное время квитанцию о приеме по телекоммуникационным каналам связи, копию декларации об объемах розничной продажи алкогольной и спиртосодержащей продукции или протокол форматно-логического контроля копии такой декларации, она информирует Росалкогольрегулирование о данном факте с использованием информационных ресурсов Росалкогольрегулирования.

14. Датой представления копии декларации об объемах розничной продажи алкогольной продукции по телекоммуникационным каналам связи является дата ее получении, указанная в квитанции о приеме указанной копии декларации по телекоммуникационным каналам связи.

V. Заключительные положения

15. Организация, осуществляющая производство, оборот и (или) использование этилового спирта, алкогольной и спиртосодержащей продукции, индивидуальный предприниматель, орган власти субъекта РФ и Росалкогольрегулирование обеспечивают хранение деклараций и (или) копий деклараций об объемах розничной продажи алкогольной и спиртосодержащей продукции, представленных по телекоммуникационным каналам связи в соответствии с настоящим Порядком в электронном виде, в течение пяти лет.

16. Экземпляр квитанции о приеме деклараций и (или) копий деклараций об объемах розничной продажи алкогольной и спиртосодержащей продукции

по телекоммуникационным каналам связи хранится в электронном архиве органа власти субъекта РФ и Росалкогольрегулирования в течение пяти лет.

17. Экземпляр протокола форматно-логического контроля деклараций и (или) копий деклараций об объемах розничной продажи алкогольной и спиртосодержащей продукции хранится в электронном архиве органа власти субъекта РФ и Росалкогольрегулирования в течение пяти лет.

Приложение №1

к приказу № ___ от _____

Требования к электронно-цифровой подписи.

1. Технические требования к защищенному ключевому носителю:

Защищенный ключевой носитель информации представляет собой защищенное устройство, предназначенное для строгой аутентификации, безопасного хранения ключевой информации, секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами и цифровыми сертификатами. Данный носитель должен быть совместим с доверенным модулем безопасности (Trusted Security Module), выполняющим функции:

- защиты от несанкционированного доступа к компьютеру до загрузки ОС;
- регистрации событий доступа (в том числе несанкционированного) к компьютеру;
- контроля целостности программной среды компьютера.

Программное обеспечение носителя ключевой информации должно обеспечивать возможность контроля длины и качества задаваемого пользователем PIN-кода и запрета использования "слабых" комбинаций с позиций качества используемых символов PIN- кода (нулевых, повторяющихся, циклических с короткими циклами и т.п.) и реализована возможность изменения параметров безопасности PIN-кода (длина, используемые символы и т.п.)

Программное обеспечение носителя ключевой информации должно обеспечивать возможность разблокирования ключевых носителей, заблокированных при исчерпании количества попыток неправильного ввода PIN-кода и возможность приведения исправных, возможно заблокированных,

ключевых носителей в первоначальное обезличенное состояние. Должна обеспечиваться возможность проведения этой операции удаленно самим пользователем с помощью системы управления ключевыми носителями.

2. Требования к аппаратной платформе:

Носитель ключевой информации должен соответствовать следующим требованиям к аппаратной платформы:

- Микросхема смарт-карты Atmel AT90SC25672RCT-USB или аналог
- Объем защищенной памяти не менее 72 КБ

Форм факторы носителя ключевой информации:

- USB-ключ.

3. Технические требования к носителю ключевой информации:

- Корпус: Не допускающий необнаружимого вскрытия
- Рабочая температура: 0°C – 70°C
- Температура хранения: -40°C – 85°C
- Влажностный режим: 0-100% без конденсата
- Срок хранения данных в памяти: Не менее 10 лет
- Среднее время наработки на отказ электронных компонентов не менее 10 лет.
- Количество циклов перезаписи памяти: Не менее 500,000

4. Требования к поддерживаемым интерфейсам и стандартам:

- PKCS#11: v2.01,
- CAPI,
- PC/CS (команды APDU),
- хранение сертификатов X.509 v3,
- SSL v3,
- IPSec/IKE;
- Microsoft CCID;
- Microsoft Smartcard Minidriver

5. Требования к аппаратно-реализованным криптографическим алгоритмам:

- RSA 1024/2048,
- DES,
- Triple DES,
- SHA1
- DH

6. Требования к поддерживаемым платформам:

- Microsoft Windows 2003/XP/Vista/2008/2008 R2/7 (32 и 64-битные версии);
- Linux;
- Mac OS

7. Требования к сертификации ключевого носителя:

Носитель ключевой информации должен иметь сертификат соответствия ФСТЭК России – как программно-аппаратное средство аутентификации и хранения ключевой информации пользователей в автоматизированных системах, обрабатывающих конфиденциальную информацию.

8. Требования к совместимости со средствами криптографической защиты информации:

- Домен-КС2
- Крипто-Про CSP

9. Требования к составу сертификата

Термины

C – country – страна

CN – common name – поле в DN – общее имя = ФИО или псевдоним.

DN – distinguished name – расширение в СКП, в которое помещается отличительное имя владельца СКП, состоящее из нескольких полей.

E – e-mail – поле в DN – электронная почта.

L – locality – место расположения, например, город.

O – organization – поле в DN – организация.

OU – organization unit – поле в DN – подразделение организации.

S – state or province – область, регион.

T – title – должность,

UN – unstructured name – поле в DN – неструктурированное имя.

INN – поле в DN – ИНН - индивидуальный номер налогоплательщика.

ИНН – индивидуальный номер налогоплательщика.

КПП – код причи ны постано вки на уч т в налоговом органе.

ИП – индивидуальный предприниматель.

СКП – сертификат ключа подписи.

СОС (CRL) – список отозванных сертификатов.

УЦ – удостоверяющий центр.

ФИО – фамилия имя отчество.

ЮЛ – юридическое лицо.

ЭЦП – электронная цифровая подпись.

Требования к СКП

Ключевая пара СКП должна соответствовать стандарту ГОСТ Р 34.10-2001.

Поля СКП должны заполняться в соответствии рекомендациям IETF RFC5280 и ITU-T x.509 (если не указано другое).

Для любого текста, используемого в СКП, разрешается использовать набор символов из Приложение 10 (если не указано другое).

Каждый СКП должен содержать следующие атрибуты и расширения:

1. Версия СКП (version) – должна быть не ниже 3.

2. Серийный номер (serialNumber) – уникальная последовательность в рамках одного УЦ, не более 160 бит.

3. Алгоритм подписи (signature) – в поле algorithm должен содержаться идентификатор алгоритма подписи ГОСТ Р 34.11-94/34.10-2001 (OID.1.2.643.2.2.3, в соответствии с RFC4491).

4. DN издателя СКП (issuer) – данные из поля субъект СКП издателя.

Для Корневого СКП значение DN издателя должно быть равно DN субъекта.

5. Дата и время начала действия СКП (notBefore).

6. Дата и время окончания действия СКП (notAfter).

7. В DN субъекта СКП (subject) должны быть заполнены поля:

7.1. CN (OID.2.5.4.3) – обязательно к заполнению – должно быть записано ФИО владельца СКП (Приложение 1).

7.2. INN (OID.1.2.643.3.131.1.1) – обязательно к заполнению. Должен быть записан один из вариантов:

- ИНН организации, сотрудником которой является владелец СКП (10 цифр в кодировке Windows-1251).
- ИНН физического лица владельца СКП, являющегося индивидуальным предпринимателем (12 цифр в кодировке Windows-1251).

7.3. UN (1.2.840.113549.1.9.2) – обязательно к заполнению. Должен быть записан один из вариантов:

- для ЮЛ должны присутствовать 4 символа КПП= и далее 9 цифр КПП организации, сотрудником которого является владелец СКП (Приложение 2).
- для ИП должны присутствовать только 4 символа КПП=.

7.4. OU (OID.2.5.4.11) – не обязательно к заполнению. Может быть записано:

- для ЮЛ подразделение организации, сотрудником которого является владелец СКП (Приложение 3).

7.5. E (OID.1.2.840.113549.1.9.1) – обязательно к заполнению. Должен быть записан:

- действующий адрес электронной почты владельца СКП (Приложение 4).

7.6. O (OID.2.5.4.10) – обязательно к заполнению. Должно быть записано:

- для ЮЛ или ИП краткое название ЮЛ или ИП – владельца СКП в соответствии с ЕГРЮЛ или ЕГРИП (Приложение 5).

7.7. C (OID.2.5.4.6) – обязательно к заполнению – должен быть записан двух символьный код страны, две прописные латинские буквы в соответствии с ISO 3166 (ISO 3166-1 alpha-2).

7.8. L (OID.2.5.4.7) – обязательно к заполнению. Должно быть записано:

- название города или населенного пункта, где зарегистрированы ЮЛ или ИП (Приложение 6).

7.9. S (OID.2.5.4.8) – обязательно к заполнению. Должно быть записано:

- название региона (субъекта Российской Федерации), где зарегистрированы ЮЛ или ИП (Приложение 7).

7.10. T (OID.2.5.4.12) – обязательно к заполнению. Должно быть записано один из вариантов:

- для ЮЛ - должность владельца СКП.
- для ИП - Индивидуальный предприниматель. (Приложение 9)

Примечание. Каждое поле в DN, описанное в п.п. 7.1 – 7.10 (кроме п.п. 7.3) допускается использовать только 1 раз. УЦ могут использовать дополнительные поля, если это не противоречит RFC, однако эти поля не будут обрабатываться в РАР.

8. Открытый ключ (subjectPublicKeyInfo):

8.1. Атрибут AlgorithmIdentifier поле algorithm – идентификатор алгоритма открытого ключа по ГОСТ Р 34.10-2001 (OID.1.2.643.2.2.19, в соответствии с RFC4491).

8.2. Атрибут AlgorithmIdentifier поле parameters – два параметра с OID.1.2.643.2.2.36.0 и OID.1.2.643.2.2.30.1 (в соответствии с RFC4491).

8.3. Атрибут subjectPublicKey – открытый ключ.

9. Расширение extKeyUsage (OID.2.5.29.37) – расширенное использование ключа – должно содержать идентификаторы использования:

«Защищенная электронная почта» (OID.1.3.6.1.5.5.7.3.4);

«Система декларирования ФСРАР» (OID. 1.2.643.5.1.28.2);

«Система декларирования ФСРАР-розничная АП» (OID. 1.2.643.5.1.28.3).

Для организаций, являющихся лицензиатами Росалкогольрегулирования или лицензиатами органов государственной власти субъектов Российской Федерации на розничную продажу алкогольной продукции должен содержаться OID «Система декларирования ФСРАР-лицензиат» (OID. 1.2.643.5.1.28.4);

Так же сюда могут быть добавлены другие идентификаторы использования по усмотрению УЦ, но при этом это расширение должно содержать не более 10 элементов.

10. Расширение subjectKeyIdentifier (OID.2.5.29.14) – идентификатор ключа субъекта – должно содержать идентификатор открытого ключа в СКП в виде уникальной последовательности, формируемой в соответствие с RFC.

11. Расширение authorityKeyIdentifier (OID.2.5.29.35 или OID.2.5.29.1) – идентификатор ключа центра сертификатов – должно быть заполнено поле keyIdentifier значением расширения subjectKeyIdentifier в СКП издателя.

Поля authorityCertIssuer и authorityCertSerialNumber могут отсутствовать в расширении, но если они заполнены, то должны содержать:

- authorityCertIssuer – DN Субъекта из СКП Издателя.
- authorityCertSerialNumber – Серийный номер из СКП издателя.

12. Расширение keyUsage (OID.2.5.29.15) – использование ключа:

12.1. Должны быть установлены в 1 биты:

- 0 (цифровая подпись), 1 (неотрекаемость) и 2 (шифрование ключей);
- биты 5 (подпись СКП) и 6 (подпись СОС) должны быть установлены в 0.

12.2. Остальные биты должны заполняться в соответствии с рекомендациями RFC.

13. Расширение cRLDistributionPoints (OID.2.5.29.31) – точка распределения списка отзыва – должно содержать действительный путь к

файлу CRL (ссылка на файл в Интернет по протоколу http). По этой ссылке УЦ, выдавший СКП, должен обеспечить круглосуточный доступ к действительному файлу CRL.

Не позднее, чем за 1 час до истечения старого CRL, должен быть выпущен новый CRL и файл по ссылке в cRLDistributionPoints должен быть заменен этим новым CRL.

14. Расширение FreshestCRL (OID.2.5.29.46) – точка распределения дельты списка отзыва – должно содержать действительный путь к файлу дельты CRL (ссылка на файл в Интернет по протоколу http). По этой ссылке УЦ, выдавший СКП, должен обеспечить круглосуточный доступ к действительный файлу дельты CRL.

Примечание. Это расширение является необязательным и должно добавляться в СКП, только если УЦ выпускает дельты CRL.

Остальные расширения могут содержать любые данные в соответствии с рекомендациями IETF RFC и ITU-T.

Размер файла СКП в формате base64 с тегами не должен превышать 8000 байт.

Требования к COC

Поля COC должны заполняться в соответствии рекомендациям IETF RFC5280 и ITU-T x.509 (если не указано другое).

Размер файла COC должен быть не более 400 Кбайт.

Для любого текста, используемого в COC, разрешается использовать набор символов из Приложение 10.

Каждый COC должен содержать следующие атрибуты и расширения:

1. Версия (version) – версия должна быть 2.

2. Издатель (issuer) – данные из поля субъект СКП издателя.

3. Дата издания COC (thisUpdate).

4. Дата издания следующего COC (nextUpdate).

5. Алгоритм подписи (signature) – должен содержать идентификатор алгоритма подписи ГОСТ Р 34.11-94/34.10-2001 (OID.1.2.643.2.2.3 в соответствии с RFC4491).

6. Расширение authorityKeyIdentifier (OID.2.5.29.35 или OID.2.5.29.1) – идентификатор ключа центра сертификатов – должно быть заполнено поле keyIdentifier значением расширения subjectKeyIdentifier в СКП издателя.

Поля authorityCertIssuer и authorityCertSerialNumber могут отсутствовать в расширении, но если они заполнены, то должны содержать:

- authorityCertIssuer – DN Субъекта из СКП Издателя.
- authorityCertSerialNumber – Серийный номер из СКП издателя

7. Номер СОС cRLNumber (OID.2.5.29.20) – порядковый номер, начинающийся с 1 и увеличивающийся каждый раз на 1 при выпуске нового СОС.

Допускается формирование значения номера СОС и дельта СОС выполнять по правилу, описанному в rfc 5280: каждый последующий номер должен быть больше предыдущего и длинна номера, должна быть не более 160 бит.

8. Индикатор дельты СОС deltaCRLIndicator (OID.2.5.29.27) критическое расширение – если в СОС присутствует это расширение, то СОС считается дельтой. Должен содержать номер равный или меньший, чем номер основного СОС из расширения cRLNumber.

Остальные расширения могут содержать любые данные, сформированные в соответствии с рекомендациями IETF RFC и ITU-T.

Требования к построению цепочек доверия СКП и СОС

Цепочки доверия СКП и СОС строятся по равенствам данных в расширении subjectKeyIdentifier издателя и authorityKeyIdentifier в изданном СКП или СОС.

Если в расширении authorityKeyIdentifier содержатся заполненные поля authorityCertIssuer и authorityCertSerialNumber, то дополнительно выполняется проверка соответствия DN из поля authorityCertIssuer атрибуту issuer из СКП

издателя и соответствие серийного номера из поля authorityCertSerialNumber серийному номеру СКП издателя.

Приложение 1

Формат ФИО владельца СКП

1. ФИО владельца СКП записывается в атрибут CN (OID.2.5.4.3) поля DN субъекта СКП.

2. Длина текста не более 64 символов.

3. ФИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца (например, паспорт). Формат:

а. первое слово – Фамилия;

б. 1 пробел;

в. второе слово – Имя;

г. 1 пробел;

д. третье слово – Отчество;

е. 1 пробел (если есть еще текст после отчества);

ж. остальные слова (если есть) могут быть отнесены к отчеству, в зависимости от контекста обработки.

4. Каждое слово в тексте должно быть отделено 1 пробелом.

5. Не разрешается использовать пробел в начале и в конце текста.

6. Разрешается использовать только 1 атрибут CN в DN субъекта.

7. Разрешается использование символов из набора (Приложение 10), за исключением символов:

№	Символ	Название	Код	Код
1	(	левая скобка	0x0028	0x28
2	)	правая скобка	0x0029	0x29
3	:	двоеточие	0x003A	0x3A
4	;	точка с запятой	0x003B	0x3B
5	@	Коммерческое ат «собачка»	0x0040	0x40