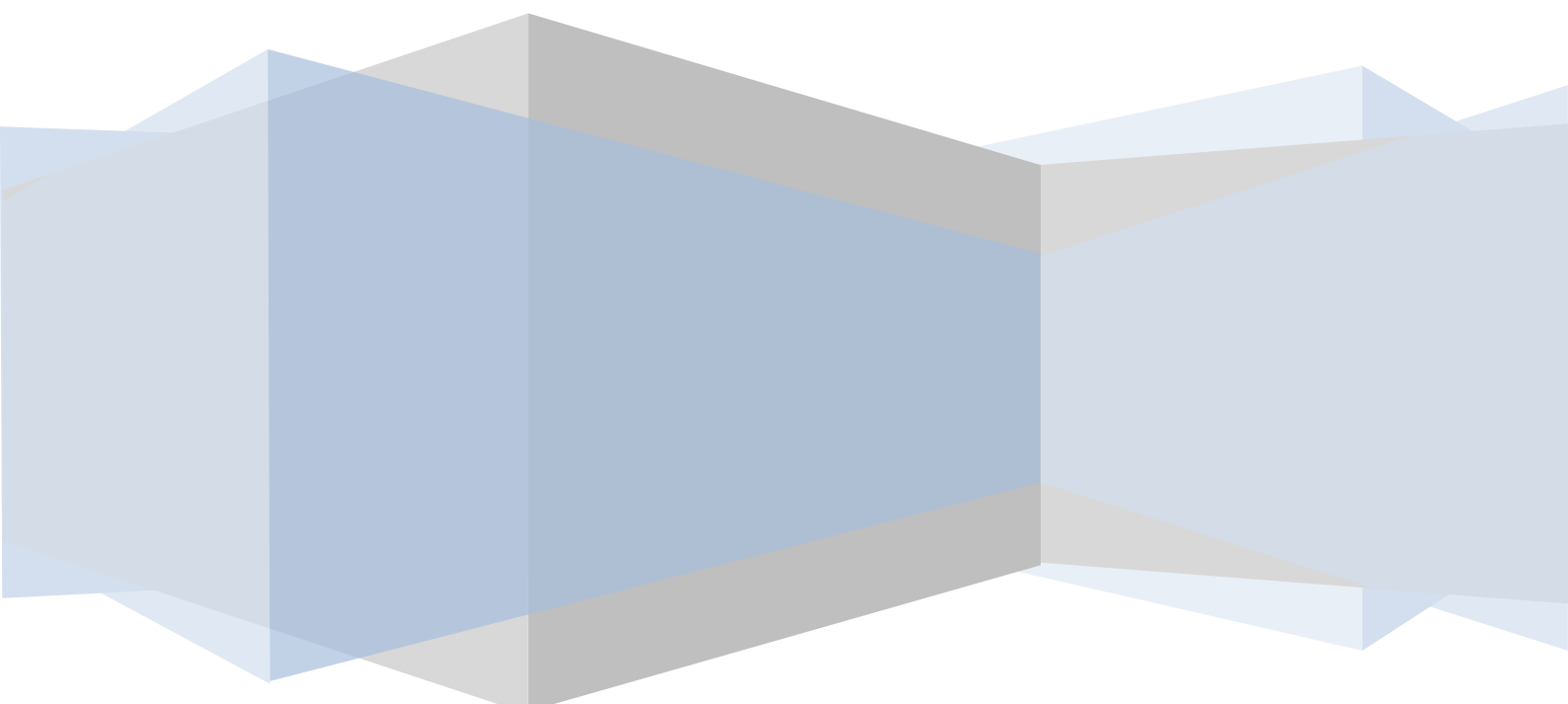


Методические рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи

Версия 1.4



1 Оглавление

2	Введение	2
2.1	Назначение документа	2
2.2	Цели и требования	2
2.3	Термины и определения	2
3	Структура сертификата	3
3.1	Общие положения.....	3
3.2	Состав СКПЭП	3
3.3	Состав имени субъекта	4
3.4	Состав имени издателя СКПЭП.....	6
Приложение 1.	Формат ФИО.....	7
Приложение 2.	Формат названия субъекта федерации.....	8
Приложение 3.	Формат названия населенного пункта.....	10
Приложение 4.	Формат наименования организации.....	10
Приложение 5.	Формат подразделения организации.....	11
Приложение 6.	Формат должности.....	12
Приложение 7.	Формат ОГРН.....	12
Приложение 8.	Формат ОГРНИП.....	12
Приложение 9.	Формат СНИЛС.....	12
Приложение 10.	Формат ИНН.....	12
Приложение 11.	Набор разрешенных символов.....	14
Приложение 12.	Дополнение «Политики сертификата».....	18
Пример сертификата УЦ		19
Приложение 13.	Пример сертификата ЮЛ (должностное лицо).....	21
Приложение 14.	Пример сертификата ЮЛ (автомат)	23
Приложение 15.	Пример сертификата ФЛ.....	25
Приложение 16.	Пример сертификата ИП	27

2 Введение

2.1 Назначение документа

Настоящий документ описывает правила формирования аккредитованными УЦ квалифицированных сертификатов ключей проверки электронной подписи, которые могут использоваться в государственных информационных системах.

2.2 Цели и требования

Данный документ разработан в целях реализации и во исполнение:

- федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- приказа ФСБ от 27 декабря 2011 г. N 795 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ФОРМЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ".

Указанные рекомендации дополняют вышеупомянутый приказ ФСБ в содержательной части состава сертификата, а так же включают в себя некоторые разъяснения.

2.3 Термины и определения

В настоящем документе используются понятия, определенные в документах, указанных в разделе «Цели и требования».

Кроме того, используются следующие сокращения:

ИНН – индивидуальный номер налогоплательщика.

ИП – индивидуальный предприниматель.

ОГРН – основной государственный регистрационный номер.

ОГРНИП – основной государственный регистрационный номер индивидуального предпринимателя.

СКПЭП – квалифицированный сертификат ключа проверки электронной подписи.

ФИО – фамилия имя отчество.

ФЛ – физическое лицо.

ЮЛ – юридическое лицо.

3 Структура сертификата

3.1 Общие положения

СКПЭП должен удовлетворять требованиям приказа ФСБ от 27 декабря 2011 г. N 795.

Для любого текста, используемого в СКПЭП, разрешается использовать набор символов, который описывает Приложение 11 (если не указано другое).

3.2 Состав СКПЭП

Каждый СКПЭП должен содержать следующие атрибуты и расширения (в указанном порядке):

1. Версия (version) – должна быть не ниже 3.
2. Серийный номер (serial number).
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. Имя издателя СКПЭП (issuer) – данные из поля «Имя владельца» соответствующего СКПЭП УЦ. См. 3.4 Состав имени издателя СКПЭП.
5. Дата и время начала действия СКПЭП (notBefore).
6. Дата и время окончания действия СКПЭП (notAfter).
7. Имя владельца СКЭП (subject). См. 3.3 Состав имени субъекта.
8. Открытый ключ (subjectPublicKeyInfo).
9. Дополнения (расширения) сертификата (Extensions). Должны содержаться следующие дополнения (порядок данным документом не регламентируется):
 - 9.1. Authority Key Identifier, OID.2.5.29.35, идентификатор ключа УЦ.
 - 9.2. Key Usage, OID.2.5.29.15, область использования ключа.
 - 9.3. Certificate Policies, OID.2.5.29.32, политики сертификата (см. Приложение 12).
 - 9.4. Subject Sign Tool, OID.1.2.643.100.111, средство ЭП владельца сертификата.
 - 9.5. Issuer Sign Tool, OID.1.2.643.100.112, средство ЭП УЦ.
 - 9.6. ExtendedKeyUsage, OID.2.5.29.37, расширенное использования ключа. Состав дополнения зависит от информационной системы, в которой используется СКПЭП.
 - 9.7. CDP, OID.2.5.29.31, точки распространения списков отзыва.

Кроме того, СКПЭП может содержать другие дополнения (не критические), в зависимости от требований конкретных информационных систем, в которых они используются.

3.3 Состав имени субъекта

Обязательными полями имени субъекта являются следующие:

Обозначение	OID	Наименование	Макс. длина	Значение	Формат
CN	2.5.4.3	Общее имя	64	ЮЛ: В зависимости от типа конечного владельца СКПЭП: - наименование организации; - ФИО должностного лица; - название автоматизированной системы; - другое отображаемое имя по требованиям информационной системы. ФЛ: ФИО	ФИО: Приложение 1 Остальные значения: нет определенного формата
C	2.5.4.6	Страна	2	Двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997)	
S	2.5.4.8	Регион	128	Наименование субъекта РФ: ЮЛ: По адресу местонахождения ФЛ: По адресу регистрации	Приложение 2
L	2.5.4.7	Населенный пункт	128	Наименование населенного пункта: ЮЛ: По адресу местонахождения ФЛ: По адресу регистрации	Приложение 3
O	2.5.4.10	Организация	64	Полное или сокращенное наименование организации (только для ЮЛ)	Приложение 4
OU	2.5.4.11	Подразделение	64	ЮЛ: В случае выпуска СКПЭП на должностное лицо – соответствующее подразделение организации	Приложение 5
T	2.5.4.12	Должность	64	ЮЛ: В случае выпуска СКПЭП на должностное лицо – его должность	Приложение 6
OGRN	1.2.643.100.1	ОГРН	13	ОГРН организации (только для ЮЛ)	Приложение 7
OGRNIP	1.2.643.100.5	ОГРНИП	15	ОГРНИП (только для ИП)	Приложение 8
SNILS	1.2.643.100.3	СНИЛС	11	ФЛ: СНИЛС ЮЛ: Не обязательно, но в случае выпуска СКПЭП на должностное лицо – данное поле строго рекомендуется включать для упрощения идентификации должностных лиц.	Приложение 9
INN	1.2.643.3.131.1.1	ИНН	12	ЮЛ/ИП: ИНН ФЛ: Не обязательно, но строго рекомендуется к включению для целей взаимодействия с ФНС.	Приложение 10

Каждое из данных обязательных полей может быть использовано только в одном экземпляре.

Порядок данным документом не регламентируется.

Кроме вышеуказанных компонент имя субъекта может включать другие поля.

3.4 Состав имени издателя СКПЭП

Обязательными полями имени субъекта являются следующие:

Обозначение	OID	Наименование	Макс. длина	Значение	Формат
CN	2.5.4.3	Общее имя	64	Псевдоним удостоверяющего центра	Нет определенного формата
C	2.5.4.6	Страна	2	Двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997)	
S	2.5.4.8	Регион	128	Наименование субъекта РФ местонахождения ПАК УЦ	Приложение 2
L	2.5.4.7	Населенный пункт	128	Наименование населенного пункта местонахождения ПАК УЦ	Приложение 3
O	2.5.4.10	Организация	64	Полное или сокращенное наименование организации	Приложение 4
OU	2.5.4.11	Подразделение	64	В случае выпуска СКПЭП на должностное лицо – соответствующее подразделение организации	Приложение 5
OGRN	1.2.643.100.1	ОГРН	13	ОГРН организации	Приложение 7
INN	1.2.643.3.131.1.1	ИНН	12	ИНН организации	Приложение 10

Каждое из данных обязательных полей может быть использовано только в одном экземпляре.

Порядок данным документом не регламентируется.

Кроме вышеуказанных компонент имя субъекта может включать другие поля.

Приложение 1. Формат ФИО.

1. 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 (если имеется);
 - е. 1 пробел (если есть еще текст после отчества);
2. Если в фамилии, имени или отчестве в написании присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов (например: Салтыков-Щедрин).
3. Если фамилия, имя или отчество состоит из нескольких слов разделенных пробелом, то в сертификат вносится одним словом, части которого соединены «подчеркиванием» без пробелов (например: фамилия «Ван чо» будет записана Ван_чо).
4. Фамилия, имя и отчество (если имеется) должны разделяться 1 пробелом.
5. Не разрешается использовать пробел в начале и в конце текста.
6. Разрешается использование символов из набора (Приложение 11), за исключением символов:

№	Символ	Название	Код UNICODE	Код Windows-1251
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
6	"	универсальная кавычка	0x0022	0x22
7	%	процент	0x0025	0x25
8	&	амперсанд	0x0026	0x26
9	+	знак плюс	0x002B	0x2B
10	№	знак номер	0x00B9	0xB9

Приложение 2. Формат названия субъекта Федерации.

1. Формат:
 - первое слово – номер региона (см. Справочник кодов регионов), 2 цифры, лидирующий ноль указывать обязательно;
 - 1 пробел;
 - остальной текст – название региона с заглавной буквы.
2. Каждое слово в тексте должно быть отделено 1 пробелом.
3. Не разрешается использовать пробел в начале и в конце текста.
4. Разрешается использование символов из набора (Приложение 11).

Справочник кодов регионов

В справочнике субъекты федерации идут в том же порядке и с теми же названиями, что и в статье 65 Конституции Российской Федерации: республики, края, области, города федерального значения, автономные области, автономные округа, дополнительные. Нумерация кодов субъектов федерации соответствует перечню по тексту статьи 71 Конституции РСФСР 1978 года в редакции от 10 ноября 1992.

Код	Название региона
01	Республика Адыгея (Адыгея)
02	Республика Башкортостан
03	Республика Бурятия
04	Республика Алтай
05	Республика Дагестан
06	Республика Ингушетия
07	Кабардино-Балкарская Республика
08	Республика Калмыкия
09	Карачаево-Черкесская Республика
10	Республика Карелия
11	Республика Коми
12	Республика Марий Эл
13	Республика Мордовия
14	Республика Саха (Якутия)
15	Республика Северная Осетия – Алания
16	Республика Татарстан
17	Республика Тыва
18	Удмуртская Республика
19	Республика Хакасия
20	Чеченская Республика
21	Чувашская Республика – Чувашия
22	Алтайский край
23	Краснодарский край

24	Красноярский край
25	Приморский край
26	Ставропольский край
27	Хабаровский край
28	Амурская область
29	Архангельская область и Ненецкий автономный округ
30	Астраханская область
31	Белгородская область
32	Брянская область
33	Владимирская область
34	Волгоградская область
35	Вологодская область
36	Воронежская область
37	Ивановская область
38	Иркутская область
39	Калининградская область
40	Калужская область
41	Камчатский край
42	Кемеровская область
43	Кировская область
44	Костромская область
45	Курганская область
46	Курская область
47	Ленинградская область
48	Липецкая область
49	Магаданская область
50	Московская область
51	Мурманская область
52	Нижегородская область
53	Новгородская область
54	Новосибирская область
55	Омская область
56	Оренбургская область
57	Орловская область
58	Пензенская область
59	Пермский край
60	Псковская область
61	Ростовская область
62	Рязанская область
63	Самарская область
64	Саратовская область
65	Сахалинская область
66	Свердловская область
67	Смоленская область
68	Тамбовская область

69	Тверская область
70	Томская область
71	Тульская область
72	Тюменская область
73	Ульяновская область
74	Челябинская область
75	Забайкальский край
76	Ярославская область
77	г. Москва
78	г. Санкт-Петербург
79	Еврейская автономная область
86	Ханты-Мансийский автономный округ – Югра
87	Чукотский автономный округ
89	Ямало-Ненецкий автономный округ
99	Иные территории, включая, г. Байконур

Приложение 3. Формат названия населенного пункта.

1. Каждое слово в тексте должно быть отделено 1 пробелом.
2. Не разрешается использовать пробел в начале и в конце текста.
3. Разрешается использование символов из набора (Приложение 11). При этом следующие символы разрешается использовать только в том случае, если они встречаются внутри официального названия города или населенного пункта:

№	Символ	Название	Код UNICODE	Код Windows-1251
1	'	апостроф	0x0027	0x27
2	«	двойная левая угловая кавычка	0x00AB	0xAB
3	»	двойная правая угловая кавычка	0x00BB	0xBB
4	"	универсальная кавычка	0x0022	0x22
5	%	процент	0x0025	0x25
6	&	амперсанд	0x0026	0x26
7	+	знак плюс	0x002B	0x2B
8	№	знак номер	0x00B9	0xB9

Приложение 4. Формат наименования организации.

1. Каждое слово в тексте должно быть отделено 1 пробелом.
2. Не разрешается использовать пробел в начале и в конце текста.

3. Разрешается использование символов из набора (Приложение 11). При этом, следующие символы разрешается использовать только в том случае, если они встречаются внутри официального названия организации:

№	Символ	Название	Код UNICODE	Код Windows-1251
1	'	апостроф	0x0027	0x27
2	«	двойная левая угловая кавычка	0x00AB	0xAB
3	»	двойная правая угловая кавычка	0x00BB	0xBB

Приложение 5. Формат подразделения организации.

1. Каждое слово в тексте должно быть отделено 1 пробелом.
2. Не разрешается использовать пробел в начале и в конце текста.
3. Разрешается использование символов из набора (Приложение 11). При этом, следующие символы разрешается использовать только в том случае, если они встречаются внутри официального названия подразделения организации:

№	Символ	Название	Код UNICODE	Код Windows-1251
1	'	апостроф	0x0027	0x27
2	«	двойная левая угловая кавычка	0x00AB	0xAB
3	»	двойная правая угловая кавычка	0x00BB	0xBB

Приложение 6. Формат должности.

1. Каждое слово в тексте должно быть отделено 1 пробелом.
2. Не разрешается использовать пробел в начале и в конце текста.
3. Разрешается использование символов из набора (Приложение 11). При этом следующие символы разрешается использовать только в том случае, если они встречаются внутри официального названия должности владельца СКПЭП:

№	Символ	Название	Код UNICODE	Код Windows-1251
1	'	апостроф	0x0027	0x27
2	«	двойная левая угловая кавычка	0x00AB	0xAB
3	»	двойная правая угловая кавычка	0x00BB	0xBB

Приложение 7. Формат ОГРН.

1. Текст длиной 13 цифр.
2. ОГРН юридического лица всегда должен присутствовать.
3. Не разрешается использовать пробел в начале и в конце текста.

Приложение 8. Формат ОГРНИП.

1. Текст длиной 15 цифр.
2. Не разрешается использовать пробел в начале и в конце текста.

Приложение 9. Формат СНИЛС.

1. Текст длиной 11 цифр.
2. При отсутствии СНИЛС у физического лица значением должны быть 11 нулей.

Примечание. Необходимо отметить, что наличие СНИЛС в сертификате физического лица является необходимым для регистрации данного физического лица в Единой системе идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме (Постановление Правительства Российской Федерации от 28 ноября 2011г. № 977). В связи с этим, строго рекомендуется заполнять поле СНИЛС.

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

Приложение 10. Формат ИНН.

1. Текст длиной 12 цифр.
2. Для ЮЛ должен содержать два лидирующих нуля, например «007707049388».

3. При отсутствии идентификатора ИНН у юридического лица значением должны быть 12 нулей.
4. Не разрешается использовать пробел в начале и в конце текста.

Примечание. Необходимо отметить, что наличие ИНН в сертификате физического лица является необходимым для подписания документов, передаваемых в ФНС в электронном виде. В связи с этим, строго рекомендуется заполнять поле ИНН.

Приложение 11. Набор разрешенных символов.

В СКПЭП любой используемый русскоязычный текст должен быть представлен в формате UNICODE, где каждый символ кодируется двумя байтами (16 бит). Для непосредственной записи в СКПЭП текст должен быть закодирован по стандарту UTF-8 (RFC 3629).

При наборе текста для СКПЭП разрешается использовать только символы, UNICODE коды которых приведены в таблице.

При извлечении и декодировании текста из СКПЭП для дальнейшей его обработки в программном обеспечении (в том числе и в ПО СИОЭД) код каждого символа должен быть дополнительно приведен к однобайтовому коду (8 бит) в кодовой странице Windows-1251, в соответствии с кодами в таблице.

Символы, UNICODE коды которых не соответствуют таблице, приведенной ниже, использовать **не разрешается**.

Набор разрешенных символов для текстов в СКПЭП

(все коды даны в шестнадцатеричной системе счисления)

№	Символ	Название	Код UNICODE	Код Windows-1251
1		пробел	0x0020	0x20
2	"	универсальная кавычка	0x0022	0x22
3	%	процент	0x0025	0x25
4	&	амперсанд	0x0026	0x26
5	'	апостроф	0x0027	0x27
6	(левая скобка	0x0028	0x28
7)	правая скобка	0x0029	0x29
8	+	знак плюс	0x002B	0x2B
9	,	запятая	0x002C	0x2C
10	-	дефис	0x002D	0x2D
11	.	точка	0x002E	0x2E
12	0	цифра ноль	0x0030	0x30
13	1	цифра один	0x0031	0x31
14	2	цифра два	0x0032	0x32
15	3	цифра три	0x0033	0x33
16	4	цифра четыре	0x0034	0x34
17	5	цифра пять	0x0035	0x35
18	6	цифра шесть	0x0036	0x36
19	7	цифра семь	0x0037	0x37
20	8	цифра восемь	0x0037	0x37
21	9	цифра девять	0x0039	0x39
22	:	двоеточие	0x003A	0x3A
23	;	точка с запятой	0x003B	0x3B

24	@	коммерческое ат «собачка»	0x0040	0x40
25	A	латинская заглавная буква A	0x0041	0x41
26	B	латинская заглавная буква B	0x0042	0x42
27	C	латинская заглавная буква C	0x0043	0x43
28	D	латинская заглавная буква D	0x0044	0x44
29	E	латинская заглавная буква E	0x0045	0x45
30	F	латинская заглавная буква F	0x0046	0x46
31	G	латинская заглавная буква G	0x0047	0x47
32	H	латинская заглавная буква H	0x0048	0x48
33	I	латинская заглавная буква I	0x0049	0x49
34	J	латинская заглавная буква J	0x004A	0x4A
35	K	латинская заглавная буква K	0x004B	0x4B
36	L	латинская заглавная буква L	0x004C	0x4C
37	M	латинская заглавная буква M	0x004D	0x4D
38	N	латинская заглавная буква N	0x004E	0x4E
39	O	латинская заглавная буква O	0x004F	0x4F
40	P	латинская заглавная буква P	0x0050	0x50
41	Q	латинская заглавная буква Q	0x0051	0x51
42	R	латинская заглавная буква R	0x0052	0x52
43	S	латинская заглавная буква S	0x0053	0x53
44	T	латинская заглавная буква T	0x0054	0x54
45	U	латинская заглавная буква U	0x0055	0x55
46	V	латинская заглавная буква V	0x0056	0x56
47	W	латинская заглавная буква W	0x0057	0x57
48	X	латинская заглавная буква X	0x0058	0x58
49	Y	латинская заглавная буква Y	0x0059	0x59
50	Z	латинская заглавная буква Z	0x005A	0x5A
51	_	подчеркивание	0x005F	0x5F
52	a	латинская строчная буква a	0x0061	0x61
53	b	латинская строчная буква b	0x0062	0x62
54	c	латинская строчная буква c	0x0063	0x63
55	d	латинская строчная буква d	0x0064	0x64
56	e	латинская строчная буква e	0x0065	0x65
57	f	латинская строчная буква f	0x0066	0x66
58	g	латинская строчная буква g	0x0067	0x67
59	h	латинская строчная буква h	0x0068	0x68
60	i	латинская строчная буква i	0x0069	0x69
61	j	латинская строчная буква j	0x006A	0x6A
62	k	латинская строчная буква k	0x006B	0x6B
63	l	латинская строчная буква l	0x006C	0x6C
64	m	латинская строчная буква m	0x006D	0x6D
65	n	латинская строчная буква n	0x006E	0x6E
66	o	латинская строчная буква o	0x006F	0x6F
67	p	латинская строчная буква p	0x0070	0x70
68	q	латинская строчная буква q	0x0071	0x71

69	r	латинская строчная буква r	0x0072	0x72
70	s	латинская строчная буква s	0x0073	0x73
71	t	латинская строчная буква t	0x0074	0x74
72	u	латинская строчная буква u	0x0075	0x75
73	v	латинская строчная буква v	0x0076	0x76
74	w	латинская строчная буква w	0x0077	0x77
75	x	латинская строчная буква x	0x0078	0x78
76	y	латинская строчная буква y	0x0079	0x79
77	z	латинская строчная буква z	0x007A	0x7A
78	Ё	кириллическая заглавная буква Ё	0x0401	0xA8
79	«	двойная левая угловая кавычка	0x00AB	0xAB
80	ё	кириллическая строчная буква ё	0x0451	0xB8
81	№	знак номер	0x00B9	0xB9
82	»	двойная правая угловая кавычка	0x00BB	0xBB
83	А	кириллическая заглавная буква А	0x0410	0xC0
84	Б	кириллическая заглавная буква Б	0x0411	0xC1
85	В	кириллическая заглавная буква В	0x0412	0xC2
86	Г	кириллическая заглавная буква Г	0x0413	0xC3
87	Д	кириллическая заглавная буква Д	0x0414	0xC4
88	Е	кириллическая заглавная буква Е	0x0415	0xC5
90	Ж	кириллическая заглавная буква Ж	0x0416	0xC6
91	З	кириллическая заглавная буква З	0x0417	0xC7
92	И	кириллическая заглавная буква И	0x0418	0xC8
93	Й	кириллическая заглавная буква Й	0x0419	0xC9
94	К	кириллическая заглавная буква К	0x041A	0xCA
95	Л	кириллическая заглавная буква Л	0x041B	0xCB
96	М	кириллическая заглавная буква М	0x041C	0xCC
97	Н	кириллическая заглавная буква Н	0x041D	0xCD
98	О	кириллическая заглавная буква О	0x041E	0xCE
99	П	кириллическая заглавная буква П	0x041F	0xCF
100	Р	кириллическая заглавная буква Р	0x0420	0xD0
101	С	кириллическая заглавная буква С	0x0421	0xD1
102	Т	кириллическая заглавная буква Т	0x0422	0xD2
103	У	кириллическая заглавная буква У	0x0423	0xD3
104	Ф	кириллическая заглавная буква Ф	0x0424	0xD4
105	Х	кириллическая заглавная буква Х	0x0425	0xD5
106	Ц	кириллическая заглавная буква Ц	0x0426	0xD6
107	Ч	кириллическая заглавная буква Ч	0x0427	0xD7
108	Ш	кириллическая заглавная буква Ш	0x0428	0xD8
109	Щ	кириллическая заглавная буква Щ	0x0429	0xD9
110	Ъ	кириллическая заглавная буква Ъ	0x042A	0xDA
111	Ы	кириллическая заглавная буква Ы	0x042B	0xDB
112	Ь	кириллическая заглавная буква Ь	0x042C	0xDC
113	Э	кириллическая заглавная буква Э	0x042D	0xDD
114	Ю	кириллическая заглавная буква Ю	0x042E	0xDE

115	Я	кириллическая заглавная буква Я	0x042F	0xDF
116	а	кириллическая строчная буква а	0x0430	0xE0
117	б	кириллическая строчная буква б	0x0431	0xE1
118	в	кириллическая строчная буква в	0x0432	0xE2
119	г	кириллическая строчная буква г	0x0433	0xE3
120	д	кириллическая строчная буква д	0x0434	0xE4
121	е	кириллическая строчная буква е	0x0435	0xE5
122	ж	кириллическая строчная буква ж	0x0436	0xE6
123	з	кириллическая строчная буква з	0x0437	0xE7
124	и	кириллическая строчная буква и	0x0438	0xE8
125	й	кириллическая строчная буква й	0x0439	0xE9
126	к	кириллическая строчная буква к	0x043A	0xEA
127	л	кириллическая строчная буква л	0x043B	0xEB
128	м	кириллическая строчная буква м	0x043C	0xEC
129	н	кириллическая строчная буква н	0x043D	0xED
130	о	кириллическая строчная буква о	0x043E	0xEE
131	п	кириллическая строчная буква п	0x043F	0xEF
132	р	кириллическая строчная буква р	0x0440	0xF0
133	с	кириллическая строчная буква с	0x0441	0xF1
134	т	кириллическая строчная буква т	0x0442	0xF2
135	у	кириллическая строчная буква у	0x0443	0xF3
136	ф	кириллическая строчная буква ф	0x0444	0xF4
137	х	кириллическая строчная буква х	0x0445	0xF5
138	ц	кириллическая строчная буква ц	0x0446	0xF6
139	ч	кириллическая строчная буква ч	0x0447	0xF7
140	ш	кириллическая строчная буква ш	0x0448	0xF8
141	щ	кириллическая строчная буква щ	0x0449	0xF9
142	ъ	кириллическая строчная буква ъ	0x044A	0xFA
143	ы	кириллическая строчная буква ы	0x044B	0xFB
144	ь	кириллическая строчная буква ь	0x044C	0xFC
145	э	кириллическая строчная буква э	0x044D	0xFD
146	ю	кириллическая строчная буква ю	0x044E	0xFE
147	я	кириллическая строчная буква я	0x044F	0xFF

Приложение 12. Дополнение «Политики сертификата».

В соответствии с приказом ФСБ от 27 декабря 2011 г. N 795:

1. Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующие идентификаторы:

- 1.2.643.100.113.1 - класс средства ЭП КС1,
- 1.2.643.100.113.2 - класс средства ЭП КС2,
- 1.2.643.100.113.3 - класс средства ЭП КС3,
- 1.2.643.100.113.4 - класс средства ЭП КВ1,
- 1.2.643.100.113.5 - класс средства ЭП КВ2,
- 1.2.643.100.113.6 - класс средства ЭП КА1.

2. Сведения о классе средств ЭП владельца квалифицированного сертификата должны быть указаны в дополнении certificatePolicies путем включения следующих идентификаторов:

- для класса средств ЭП КС1: 1.2.643.100.113.1,
- для класса средств ЭП КС2: 1.2.643.100.113.1, 1.2.643.100.113.2,
- для класса средств ЭП КС3: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3,
- для класса средств ЭП КВ1: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4,
- для класса средств ЭП КВ2: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4, 1.2.643.100.113.5,
- для класса средств ЭП КА1: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4, 1.2.643.100.113.5, 1.2.643.100.113.6.

Для средств ЭП, класс которых отличается от класса средств УЦ, в которых используются указанные средства ЭП, следует указывать идентификаторы для класса средств ЭП, соответствующего классу средств УЦ.

Помимо идентификаторов политик, описывающих класс ЭП владельца квалифицированного сертификата, в дополнении «Политики сертификата» могут содержаться другие описатели политик.

Пример сертификата УЦ

Версия: 3

Серийный номер: 19bc72b40002000097be

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Поставщик:

CN=УЦ ООО "Тестовая организация"

C=RU

S=77 г.Москва

L=Москва

Street=Тверская улица, дом 97

O=ООО "Тестовая организация"

OGRN=0123456789123

INN=000123456789

NotBefore: 01.02.2012 14:43

NotAfter: 01.02.2017 14:43

Субъект:

CN=УЦ ООО "Тестовая организация"

C=RU

S=77 г.Москва

L=Москва

Street=Тверская улица, дом 97

O=ООО "Тестовая организация"

OGRN=0123456789123

INN=000123456789

Алгоритм открытого ключа:

ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001

Параметры алгоритма:

0000 30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03

0010 02 02 1e 01

1.2.643.2.2.35.1 ГОСТ Р 34.10-2001, параметры по умолчанию

1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию

Длина открытого ключа: 512 бит

Открытый ключ: UnusedBits = 0

0000 04 40 e6 b4 de f1 c7 b2 b3 1c 5e 1a f8 75 50 16

0010 a7 f9 f4 c6 96 27 68 64 16 00 b3 9c 0f 52 9b 3c

0020 02 b4 54 4c ab 8f ac 7f 16 94 59 59 e0 71 42 ce

0030 71 f7 65 c2 c4 8e 60 99 85 b3 b7 39 23 d1 fe af

0040 4b 00

Расширения сертификатов: 4

2.5.29.15: Флаги = 0, Длина = 4

Использование ключа

Цифровая подпись, Подписывание сертификатов, Автономное
подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (86)

2.5.29.19: Флаги = 1 (Критический), Длина = 5

Основные ограничения

Тип субъекта=ЦС

Ограничение на длину пути=Отсутствует

2.5.29.14: Флаги = 0, Длина = 16

Идентификатор ключа субъекта

25 d3 e9 71 b7 d6 04 70 89 f6 bf e2 64 10 2f f9 6c ca 06 d1

1.3.6.1.4.1.311.21.1: Флаги = 0, Длина = 3

Версия ЦС

V0.0

2.5.29.32: Флаги = 0

Политики сертификата

[1] Политика сертификата:

Идентификатор политики=Класс средств УЦ КС2

[2] Политика сертификата:

Идентификатор политики=Класс средства ЭП КС1

[3] Политика сертификата:

Идентификатор политики=Класс средства ЭП КС2

1.2.643.100.112: Флаги = 0

Средства электронной подписи и УЦ издателя

Средство электронной подписи: Название средства ЭП

Заключение на средство ЭП: Реквизиты заключения

Средство УЦ: Название средства УЦ

Заключение на средство УЦ: Реквизиты заключения

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Подпись: НеиспользБит=0

0000 5d 57 0c a8 e4 f0 82 18 bc 2c 97 5b 2d d5 cb ee

0010 4a 80 2a 6c ca 6f d4 bd 94 c4 07 37 6e b4 98 fd

0020 e2 fb 70 48 69 62 c9 88 16 2c eb e8 5f e0 f4 7d

0030 3a ec 8f 01 fc 93 20 fb 24 09 9f 75 0d 7f bf e8

Приложение 13. Пример сертификата ЮЛ (должностное лицо)

Версия: 3

Серийный номер: 19bc72b40002000097be

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Поставщик:

CN=УЦ ООО "Тестовая организация"

C=RU

S=77 г.Москва

L=Москва

Street=Тверская улица, дом 97

O=ООО "Тестовая организация"

OGRN=0123456789123

INN=000123456789

NotBefore: 24.02.2012 07:02

NotAfter: 24.02.2013 07:02

Субъект:

CN=Иванов Иван Иванович

SN=Иванов

G=Иван Иванович

C=RU

S=69 Тверская область

L=Нижний Волочек

O=ООО "Рога и копыта"

OU=Отдел контроля

T=Инженер-аналитик

OGRN=0123456789123

SNILS=12345678909

INN=000123456789

Алгоритм открытого ключа:

ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001

Параметры алгоритма:

0000 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03

0010 02 02 1e 01

1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию

1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию

Длина открытого ключа: 512 бит

Открытый ключ: UnusedBits = 0

0000 04 40 e6 b4 de f1 c7 b2 b3 1c 5e 1a f8 75 50 16

0010 a7 f9 f4 c6 96 27 68 64 16 00 b3 9c 0f 52 9b 3c

0020 02 b4 54 4c ab 8f ac 7f 16 94 59 59 e0 71 42 ce

0030 71 f7 65 c2 c4 8e 60 99 85 b3 b7 39 23 d1 fe af

0040 4b 00

Расширения сертификатов: 10

2.5.29.15: Флаги = 1 (Критический)

Использование ключа

Цифровая подпись, Неотрекаемость, Шифрование ключей,

Шифрование данных (f0)

2.5.29.37: Флаги = 0

Улучшенный ключ

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

2.5.29.14: Флаги = 0

Идентификатор ключа субъекта

ba 62 38 46 36 fc 14 60 63 c7 69 5a d8 80 23 6f 1f 4a 79 5f

2.5.29.35: Флаги = 0

Идентификатор ключа центра сертификатов

Идентификатор ключа=6d 8f 5e 05 d9 5f ac 91 17 94 1e 95 9a 05
30 38 37 7a 10 2a

2.5.29.31: Флаги = 0

Точки распространения списков отзыва (CRL)

[1]Точка распределения списка отзыва (CRL)

Имя точки распространения:

Полное имя:

URL=http://rg-test.ru/cdp/root.crl

1.3.6.1.5.5.7.1.1: Флаги = 0

Доступ к информации о центрах сертификации

[1]Доступ к сведениям центра сертификации

Метод доступа=Поставщик центра сертификации

(1.3.6.1.5.5.7.48.2)

Дополнительное имя:

URL=http://rg-test.ru/cdp/root.cer

2.5.29.16: Флаги = 0

Период использования закрытого ключа

Действителен с 23 февраля 2012 г. 07:02:00

Действителен по 23 февраля 2013 г. 07:02:00

2.5.29.32: Флаги = 0

Политики сертификата

[1]Политика сертификата:

Идентификатор политики=Класс средств УЦ КС2

[2]Политика сертификата:

Идентификатор политики=Класс средства ЭП КС1

[3]Политика сертификата:

Идентификатор политики=Класс средства ЭП КС2

1.2.643.100.112: Флаги = 0

Средства электронной подписи и УЦ издателя

Средство электронной подписи: Название средства ЭП

Заключение на средство ЭП: Реквизиты заключения

Средство УЦ: Название средства УЦ

Заключение на средство УЦ: Реквизиты заключения

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Подпись: НеиспользБит=0

0000 5d 57 0c a8 e4 f0 82 18 bc 2c 97 5b 2d d5 cb ee

0010 4a 80 2a 6c ca 6f d4 bd 94 c4 07 37 6e b4 98 fd

0020 e2 fb 70 48 69 62 c9 88 16 2c eb e8 5f e0 f4 7d

0030 3a ec 8f 01 fc 93 20 fb 24 09 9f 75 0d 7f bf e8

Приложение 14. Пример сертификата ЮЛ (автомат)

Версия: 3

Серийный номер: 19bc72b40002000097be

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Поставщик:

CN=УЦ ООО "Тестовая организация"

C=RU

S=77 г.Москва

L=Москва

Street=Тверская улица, дом 97

O=ООО "Тестовая организация"

OGRN=0123456789123

INN=000123456789

NotBefore: 24.02.2012 07:02

NotAfter: 24.02.2013 07:02

Субъект:

CN=Почтовый сервер

C=RU

S=69 Тверская область

L=Нижний Волочек

O=ООО "Рога и копыта"

OGRN=0123456789123

INN=000123456789

Алгоритм открытого ключа:

ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001

Параметры алгоритма:

0000 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03

0010 02 02 1e 01

1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию

1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию

Длина открытого ключа: 512 бит

Открытый ключ: UnusedBits = 0

0000 04 40 e6 b4 de f1 c7 b2 b3 1c 5e 1a f8 75 50 16

0010 a7 f9 f4 c6 96 27 68 64 16 00 b3 9c 0f 52 9b 3c

0020 02 b4 54 4c ab 8f ac 7f 16 94 59 59 e0 71 42 ce

0030 71 f7 65 c2 c4 8e 60 99 85 b3 b7 39 23 d1 fe af

0040 4b 00

Расширения сертификатов: 10

2.5.29.15: Флаги = 1 (Критический)

Использование ключа

Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

2.5.29.37: Флаги = 0

Улучшенный ключ

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

2.5.29.14: Флаги = 0

Идентификатор ключа субъекта

ba 62 38 46 36 fc 14 60 63 c7 69 5a d8 80 23 6f 1f 4a 79 5f

2.5.29.35: Флаги = 0

Идентификатор ключа центра сертификатов

Идентификатор ключа=6d 8f 5e 05 d9 5f ac 91 17 94 1e 95 9a 05
30 38 37 7a 10 2a

2.5.29.31: Флаги = 0

Точки распространения списков отзыва (CRL)

[1]Точка распределения списка отзыва (CRL)

Имя точки распространения:

Полное имя:

URL=http://rg-test.ru/cdp/root.crl

1.3.6.1.5.5.7.1.1: Флаги = 0

Доступ к информации о центрах сертификации

[1]Доступ к сведениям центра сертификации

Метод доступа=Поставщик центра сертификации

(1.3.6.1.5.5.7.48.2)

Дополнительное имя:

URL=http://rg-test.ru/cdp/root.cer

2.5.29.16: Флаги = 0

Период использования закрытого ключа

Действителен с 23 февраля 2012 г. 07:02:00

Действителен по 23 февраля 2013 г. 07:02:00

2.5.29.32: Флаги = 0

Политики сертификата

[1]Политика сертификата:

Идентификатор политики=Класс средств УЦ КС2

[2]Политика сертификата:

Идентификатор политики=Класс средства ЭП КС1

[3]Политика сертификата:

Идентификатор политики=Класс средства ЭП КС2

1.2.643.100.112: Флаги = 0

Средства электронной подписи и УЦ издателя

Средство электронной подписи: Название средства ЭП

Заключение на средство ЭП: Реквизиты заключения

Средство УЦ: Название средства УЦ

Заключение на средство УЦ: Реквизиты заключения

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Подпись: НеиспользБит=0

0000 5d 57 0c a8 e4 f0 82 18 bc 2c 97 5b 2d d5 cb ee

0010 4a 80 2a 6c ca 6f d4 bd 94 c4 07 37 6e b4 98 fd

0020 e2 fb 70 48 69 62 c9 88 16 2c eb e8 5f e0 f4 7d

0030 3a ec 8f 01 fc 93 20 fb 24 09 9f 75 0d 7f bf e8

Приложение 15. Пример сертификата ФЛ

Версия: 3

Серийный номер: 19bc72b40002000097be

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Поставщик:

CN=УЦ ООО "Тестовая организация"

C=RU

S=77 г.Москва

L=Москва

Street=Тверская улица, дом 97

O=ООО "Тестовая организация"

OGRN=0123456789123

INN=000123456789

NotBefore: 24.02.2012 07:02

NotAfter: 24.02.2013 07:02

Субъект:

CN=Петров Петр Петрович

C=RU

S=69 Тверская область

L=Нижний Волочек

SNILS=12345678909

INN=123456789098

Алгоритм открытого ключа:

ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001

Параметры алгоритма:

0000 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03

0010 02 02 1e 01

1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию

1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию

Длина открытого ключа: 512 бит

Открытый ключ: UnusedBits = 0

0000 04 40 e6 b4 de f1 c7 b2 b3 1c 5e 1a f8 75 50 16

0010 a7 f9 f4 c6 96 27 68 64 16 00 b3 9c 0f 52 9b 3c

0020 02 b4 54 4c ab 8f ac 7f 16 94 59 59 e0 71 42 ce

0030 71 f7 65 c2 c4 8e 60 99 85 b3 b7 39 23 d1 fe af

0040 4b 00

Расширения сертификатов: 10

2.5.29.15: Флаги = 1 (Критический)

Использование ключа

Цифровая подпись, Неотрекаемость, Шифрование ключей,
Шифрование данных (f0)

2.5.29.37: Флаги = 0

Улучшенный ключ

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

2.5.29.14: Флаги = 0

Идентификатор ключа субъекта

ba 62 38 46 36 fc 14 60 63 c7 69 5a d8 80 23 6f 1f 4a 79 5f

2.5.29.35: Флаги = 0
Идентификатор ключа центра сертификатов
Идентификатор ключа=6d 8f 5e 05 d9 5f ac 91 17 94 1e 95 9a 05
30 38 37 7a 10 2a

2.5.29.31: Флаги = 0
Точки распространения списков отзыва (CRL)
[1]Точка распределения списка отзыва (CRL)
Имя точки распространения:
Полное имя:
URL=http://rg-test.ru/cdp/root.crl

1.3.6.1.5.5.7.1.1: Флаги = 0
Доступ к информации о центрах сертификации
[1]Доступ к сведениям центра сертификации
Метод доступа=Поставщик центра сертификации
(1.3.6.1.5.5.7.48.2)
Дополнительное имя:
URL=http://rg-test.ru/cdp/root.cer

2.5.29.16: Флаги = 0
Период использования закрытого ключа
Действителен с 23 февраля 2012 г. 07:02:00
Действителен по 23 февраля 2013 г. 07:02:00

2.5.29.32: Флаги = 0
Политики сертификата
[1]Политика сертификата:
Идентификатор политики=Класс средств УЦ КС2
[2]Политика сертификата:
Идентификатор политики=Класс средства ЭП КС1
[3]Политика сертификата:
Идентификатор политики=Класс средства ЭП КС2

1.2.643.100.112: Флаги = 0
Средства электронной подписи и УЦ издателя
Средство электронной подписи: Название средства ЭП
Заключение на средство ЭП: Реквизиты заключения
Средство УЦ: Название средства УЦ
Заключение на средство УЦ: Реквизиты заключения

Алгоритм подписи:
ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001
Параметры алгоритма: NULL

Подпись: НеиспользБит=0
0000 5d 57 0c a8 e4 f0 82 18 bc 2c 97 5b 2d d5 cb ee
0010 4a 80 2a 6c ca 6f d4 bd 94 c4 07 37 6e b4 98 fd
0020 e2 fb 70 48 69 62 c9 88 16 2c eb e8 5f e0 f4 7d
0030 3a ec 8f 01 fc 93 20 fb 24 09 9f 75 0d 7f bf e8

Приложение 16. Пример сертификата ИП

Версия: 3

Серийный номер: 19bc72b40002000097be

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Поставщик:

CN=УЦ ООО "Тестовая организация"

C=RU

S=77 г.Москва

L=Москва

Street=Тверская улица, дом 97

O=ООО "Тестовая организация"

OGRN=0123456789123

INN=000123456789

NotBefore: 24.02.2012 07:02

NotAfter: 24.02.2013 07:02

Субъект:

CN=Петров Петр Петрович

C=RU

S=69 Тверская область

L=Нижний Волочек

OGRNIP=123456789098765

SNILS=12345678909

INN=123456789098

Алгоритм открытого ключа:

ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001

Параметры алгоритма:

0000 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03

0010 02 02 1e 01

1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию

1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию

Длина открытого ключа: 512 бит

Открытый ключ: UnusedBits = 0

0000 04 40 e6 b4 de f1 c7 b2 b3 1c 5e 1a f8 75 50 16

0010 a7 f9 f4 c6 96 27 68 64 16 00 b3 9c 0f 52 9b 3c

0020 02 b4 54 4c ab 8f ac 7f 16 94 59 59 e0 71 42 ce

0030 71 f7 65 c2 c4 8e 60 99 85 b3 b7 39 23 d1 fe af

0040 4b 00

Расширения сертификатов: 10

2.5.29.15: Флаги = 1 (Критический)

Использование ключа

Цифровая подпись, Неотрекаемость, Шифрование ключей,

Шифрование данных (f0)

2.5.29.37: Флаги = 0

Улучшенный ключ

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

2.5.29.14: Флаги = 0

Идентификатор ключа субъекта

ba 62 38 46 36 fc 14 60 63 c7 69 5a d8 80 23 6f 1f 4a 79 5f

2.5.29.35: Флаги = 0

Идентификатор ключа центра сертификатов

Идентификатор ключа=6d 8f 5e 05 d9 5f ac 91 17 94 1e 95 9a 05
30 38 37 7a 10 2a

2.5.29.31: Флаги = 0

Точки распространения списков отзыва (CRL)

[1]Точка распределения списка отзыва (CRL)

Имя точки распространения:

Полное имя:

URL=http://rg-test.ru/cdp/root.crl

1.3.6.1.5.5.7.1.1: Флаги = 0

Доступ к информации о центрах сертификации

[1]Доступ к сведениям центра сертификации

Метод доступа=Поставщик центра сертификации

(1.3.6.1.5.5.7.48.2)

Дополнительное имя:

URL=http://rg-test.ru/cdp/root.cer

2.5.29.16: Флаги = 0

Период использования закрытого ключа

Действителен с 23 февраля 2012 г. 07:02:00

Действителен по 23 февраля 2013 г. 07:02:00

2.5.29.32: Флаги = 0

Политики сертификата

[1]Политика сертификата:

Идентификатор политики=Класс средств УЦ КС2

[2]Политика сертификата:

Идентификатор политики=Класс средства ЭП КС1

[3]Политика сертификата:

Идентификатор политики=Класс средства ЭП КС2

1.2.643.100.112: Флаги = 0

Средства электронной подписи и УЦ издателя

Средство электронной подписи: Название средства ЭП

Заключение на средство ЭП: Реквизиты заключения

Средство УЦ: Название средства УЦ

Заключение на средство УЦ: Реквизиты заключения

Алгоритм подписи:

ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

Параметры алгоритма: NULL

Подпись: НеиспользБит=0

0000 5d 57 0c a8 e4 f0 82 18 bc 2c 97 5b 2d d5 cb ee

0010 4a 80 2a 6c ca 6f d4 bd 94 c4 07 37 6e b4 98 fd

0020 e2 fb 70 48 69 62 c9 88 16 2c eb e8 5f e0 f4 7d

0030 3a ec 8f 01 fc 93 20 fb 24 09 9f 75 0d 7f bf e8