Требования к форматам проверяемых сертификатов и электронных документов

сертификаты

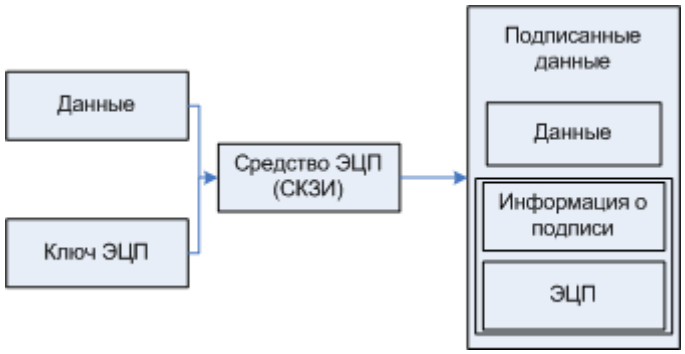
Сертификаты открытых ключей должны соответствовать требованиям, определенным приказом Министерства связи и массовых коммуникаций Российской Федерации от 23.03.2009 № 41 "Требования к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра" http://minkomsvjaz.ru/3491/766/3432/7201/7329/

электронные документы

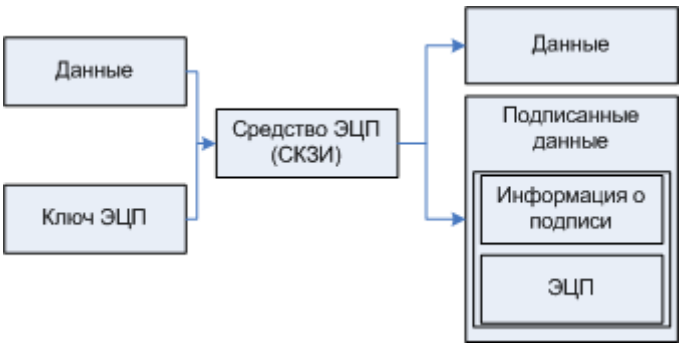
Форматы электронных документов с ЭЦП должны соответствовать требованиям PKCS#7 (CMS) (см. http://www.ietf.org/rfc/rfc3852.txt).

Сервис проверяет электронные документы двух типов, в которых:

- ЭЦП входит в состав документа (attached signature)



- ЭЦП хранится отдельно от документа (detached signature)



Подписанные данные включают в себя информацию о владельцах сертификатов, с помощью которых была сформирована подпись. Кроме этого в состав подписанных данных могут быть включены наборы сертификатов и списков отозванных сертификатов (CRL), связанные с ЭЦП.

Подписанные данные хранятся в структуре:
SignedData ::= SEQUENCE {
version CMSVersion,
digestAlgorithms DigestAlgorithmIdentifiers,
encapContentInfo EncapsulatedContentInfo,
certificates [0] IMPLICIT CertificateSet OPTIONAL,
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
signerInfos SignerInfos }

Для каждой подписи информация о подписи и атрибутах, использованных при ее создании, а так же сертификаты и списки отозванных сертификатов, связанные с данной подписью, хранятся в структуре SignerInfos:

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
version CMSVersion,
sid SignerIdentifier,
digestAlgorithm DigestAlgorithmIdentifier,
signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
signatureAlgorithm SignatureAlgorithmIdentifier,
signature SignatureValue,
unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }

Статусы сертификатов

Статус	Описание
Действителен	Сертификат действителен на текущий момент времени
Срок действия сертификата закончился или еще не наступил	Сертификат или один из сертификатов в цепочке не действителен на текущий момент времени
Сертификат имеет неверное временное вложение	Сроки действия сертификатов непересекаются
Сертификат отозван	Сертификат или один из сертификатов в цепочке

	отозван
Сертификат содержит недействительную электронную цифровую подпись	Сертификат или один из сертификатов в цепочке искажен (содержит недействительную цифровую подпись)
Сертификат не предназначен для данного использования	Сертификат или один из сертификатов в цепочке не предназначен для данного использования
Сертификат уполномоченного лица УЦ отсутствует в списке доверенных сертификатов	Сертификат или один из сертификатов в цепочке издан недоверенным цетром сертификации
Не удалось проверить статус сертификата	В сертификате или одном из сертификатов в цепочке отсутствует информация о CDP или УЦ выдавший сертификат не является доверенным
Циклическая цепочка	Один из сертификатов в цепочке издан центром, сертифицированным проверяемым сертификатом
Неверное расширение сертификата	Один из сертификатов в цепочке содержит неправильное расширение
Сертификат содержит запрещенную политику сопоставления, либо не содержит требуемую политику выдачи	Сертификат или один из сертификатов в цепочке содержит запрещенную политику сопоставления, либо не содержит требуемую политику выдачи
Нарушены основные ограничения выдачи сертификатов	Сертификат или один из сертификатов в цепочке содержит политику выдачи, которая не допускает издание сертификатов или размер цепочки исчерпан
Неверные ограничения имени	Сертификат или один из сертификатов в цепочке содержит ограничения имени, которые не выполняются
Неподдерживаемое ограничения имени	Сертификат или один из сертификатов в цепочке содержит не поддерживаемое ограничение имени
Отсутствуют требуемые ограничения имени	Сертификат или один из сертификатов в цепочке содержит ограничение имени и ограничение имени отсутствует в одном из имен в конечном сертификате
Присутствуют неразрешенные ограничения имени	Сертификат или один из сертификатов в цепочке содержит ограничение имени и в конечном сертификате содержится одно из недопустимых имен
Присутствует явно исключенные ограничения имени	Сертификат или один из сертификатов в цепочке содержит ограничение имени и в конечном одно из имен в конечном сертификате явно исключено
Информация о приостановлении или аннулировании сертификата недоступна	Информация о приостановлении или аннулировании конечного сертификата или одного из сертификатов в цепочке недоступна
Отсутствует политика выдачи	Конечный сертификат в цепочке не содержит политики выдачи и один из УЦ требует их наличия
Сертификат явно лишен доверия	Сертификат явно лишен доверия
Неподдерживаемое критическое	Сертификат или один из сертификатов в цепочке

расширение	содержит неподдерживаемое критическое расширение

Список сертификатов уполномоченных лиц аккредитованных УЦ

Список сертификатов уполномоченных лиц аккредитованных УЦ (TSL) формируется в соответствии со стандартом ETSI TS 102 231 "Provision of harmonized Trust Service Provider status information" Европейского института стандартизации в области телекоммуникаций (ETSI) и заверяется ЭЦП.
В соответствии со стандартом, список может содержать не только сертификаты уполномоченных лиц аккредитованных УЦ, а так же включать в себя описания и ссылки на другие сервисы, предоставляемые аккредитованными УЦ, к которым относятся сервисы штампов времени (TSP), сервисы онлайновой проверки статусов сертификатов (OCSP) и др.

Применение TSL должно оказать помощь пользователю при ответе на вопросы:

- предоставляет или предоставлял ли TSP защищенную услугу;
- соответствует или соответствовало ли ее предоставление критериям схемы на момент оказания услуги или на момент совершения транзакции, основанной на продуктах услуги.

Об использовании TSL списка в Евросоюзе:
http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

Описание отчета о подтверждении подлинности ЭЦП сертификата

Ниже приведен пример отчета о подтверждении подлинности ЭЦП сертификата.

Комментарии к отчету отмечены курсивом и красным цветом.

Общий результат подтверждения подлинности ЭЦП: Результат подтверждения подлинности сертификата - подлинность ПОДТВЕРЖДЕНА
Краткая форма отчета:

Статус сертификата, использованного для подтверждения подлинности ЭЦП - ДЕЙСТВИТЕЛЕН

Краткая информация по каждому из сертификатов, использованному при подтверждении подлинности:

Статусы использованных сертификатов:

Владелец сертификата:Кирьяков Кирилл Николаевич, Отдел информационных технологий, "ООО ""ПНК""", Челябинск, 74 Челябинская область, RU, kkn@y-center.ru

Действителен

Уполномоченное лицо УЦ:PNK Ltd. CA, PNK Ltd., Certification Authority, Chelyabinsk, Chelyabinskaya obl., RU, Koval LV, support@y-center.ru

Действителен

Полная форма отчета:

Отчет об установлении статуса сертификата

Время создания отчета: 28 января 2011 13:38:27 (28 января 2011 10:38:27)

Время, на которое проводилась проверка: 28 января 2011 13:38:19 (28 января 2011 10:38:19)

Серийный номер: 113F 9942 0005 0000 1559

Субъект: Кирьяков Кирилл Николаевич, Отдел информационных технологий, "ООО ""ПНК""", Челябинск, 74 Челябинская область, RU, kkn@y-center.ru

Статус сертификата подписи - ДЕЙСТВИТЕЛЕН

ЭЦП уполномоченных лиц удостоверяющих центров в цепочке сертификатов - ВЕРНА

Результат установления статуса цепочки сертификатов

Субъект: Кирьяков Кирилл Николаевич, Отдел информационных технологий, "ООО ""ПНК""", Челябинск, 74 Челябинская область, RU, kkn@y-center.ru

Поставщик: PNK Ltd. CA, PNK Ltd., Certification Authority, Chelyabinsk, Chelyabinskaya obl., RU, Koval LV, support@y-center.ru

Серийный номер: 113F 9942 0005 0000 1559

Результат установления статуса сертификата

Действителен

Информация о приостановлении действия или аннулировании сертификата (с использованием списка отозванных сертификатов):

Найдено СОС: 1

Результат проверки СОС номер 1

Поставщик: PNK Ltd. CA, PNK Ltd., Certification Authority, Chelyabinsk, Chelyabinskaya obl., RU, Koval LV, support@y-center.ru

Идентификатор ключа:

Значение:

```
12D6 28DC D5C2 DD27 DB30 F884 B584 7212 0184
0000
```

Номер СОС: 599

Действителен с:

27 января 2011 12:43:12

Действителен по:

30 января 2011 16:03:12

Статус СОС: Действителен

Информация о сертификате из списка отзыва:

```
Действителен
```

Информация о приостановлении действия или аннулировании сертификата (с использованием онлайн проверки статуса):

Найдено статусов в OCSP-ответах: 0

Субъект: PNK Ltd. CA, PNK Ltd., Certification Authority, Chelyabinsk, Chelyabinskaya obl., RU, Koval LV, support@y-center.ru

Поставщик: PNK Ltd. CA, PNK Ltd., Certification Authority, Chelyabinsk, Chelyabinskaya obl., RU, Koval LV, support@y-center.ru

Серийный номер: 0182 0940 B504 239A 424E AE6E 79D5 84CD

Результат установления статуса сертификата

```
Действителен
```

Информация по каждому из сертификатов, использованному при подтверждении

подлинности:

Сертификаты, использованные при подтверждении подлинности ЭЦП

Информация по сертификату:

Сертификат X.509:

Сведения о сертификате:

Этот сертификат:

Защищает сообщения электронной почты

Кому выдан:

Кирьяков Кирилл Николаевич

Кем выдан:

PNK Ltd. CA

Действителен с Thursday, September 02, 2010 8:49:00 AM UTC по Friday, September 02, 2011 8:58:00 AM UTC

Версия: 3 (0x2)

Серийный номер:

`113F 9942 0005 0000 1559`

Издатель:

CN = PNK Ltd. CA

O = PNK Ltd.

OU = Certification Authority

L = Chelyabinsk

S = Chelyabinskaya obl.

C = RU

T = Koval LV

E = support@y-center.ru

Срок действия:

Действителен с:

Thursday, September 02, 2010 8:49:00 AM UTC

Действителен по:

Friday, September 02, 2011 8:58:00 AM UTC

Субъект:

CN = Кирьяков Кирилл Николаевич

OU = Отдел информационных технологий

O = ООО "ПНК"

L = Челябинск

S = 74 Челябинская область

C = RU

E = kkn@y-center.ru

Открытый ключ:

Алгоритм открытого ключа:

Название:

GOST R 34.10-2001

Идентификатор:

1.2.643.2.2.19

Параметры:

```
30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
```

Значение:

```
0440 0CD1 D4E7 015C 0B14 2D17 2FE5 4DA9 BF1F
0A8F CD8A A694 32F2 EF86 41E7 AEE7 04BE 5F69
3EC0 F40E E678 9626 5A6F 6596 F196 7A07 07DE
CC7A EC46 5424 40AF 784E 2EDF
```

Расширения X.509

1. Расширение 2.5.29.15 (критическое)

Название:

Key Usage

Значение:

```
Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
```

2. Расширение 2.5.29.37

Название:

Enhanced Key Usage

Значение:

```
Secure Email (1.3.6.1.5.5.7.3.4)
```

3. Расширение 2.5.29.14

Название:

Subject Key Identifier

Значение:

```
f1 86 16 19 c9 b1 da ce 29 28 85 c7 ae 7c f3 6e b1 b8 a2 a1
```

4. Расширение 2.5.29.35

Название:

Authority Key Identifier

Значение:

```
KeyID=12 d6 28 dc d5 c2 dd 27 db 30 f8 84 b5 84 72 12 01 84 00 a1
```

5. Расширение 2.5.29.31

Название:

CRL Distribution Points

Значение:

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://ca.y-center.ru/crl_2010.crl
```

6. Расширение 1.3.6.1.5.5.7.1.1

Название:

Authority Information Access

Значение:

```
[1]Authority Info Access
     Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
     Alternative Name:
          URL=http://cs/CertEnroll/cs_PNK%20Ltd.%20CA(5).crt
[2]Authority Info Access
     Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
     Alternative Name:
          URL=file://\\cs\CertEnroll\cs_PNK%20Ltd.%20CA(5).crt
```

ЭЦП:

Алгоритм ЭЦП:

Название:

GOST R 34.11/34.10-2001

Идентификатор:

1.2.643.2.2.3

Параметры:

```
05 00
```

Значение:

```
91CF CAA7 7E20 FD13 0BF3 4E51 E5C3 829B C2EC
CE19 C8B2 DB46 9F64 1C15 8877 5FE0 04BC D25F
FC64 4CF3 DC5D CEC2 E68D 805A D4C8 6A22 AD58
7DFD 191B DE50 6C4A 0FD7
```

Информация по сертификату:

Сертификат X.509:

Сведения о сертификате:

Кому выдан:

PNK Ltd. CA

Кем выдан:

PNK Ltd. CA

Действителен с Friday, June 04, 2010 4:08:02 AM UTC по Tuesday, June 04, 2013 4:14:45

AM UTC

Версия: 3 (0x2)

Серийный номер:

0182 0940 B504 239A 424E AE6E 79D5 84CD

Издатель:

CN = PNK Ltd. CA

O = PNK Ltd.

OU = Certification Authority

L = Chelyabinsk

S = Chelyabinskaya obl.

C = RU

T = Koval LV

E = support@y-center.ru

Срок действия:

Действителен с:

Friday, June 04, 2010 4:08:02 AM UTC

Действителен по:

Tuesday, June 04, 2013 4:14:45 AM UTC

Субъект:

CN = PNK Ltd. CA

O = PNK Ltd.

OU = Certification Authority

L = Chelyabinsk

S = Chelyabinskaya obl.

C = RU

T = Koval LV

E = support@y-center.ru

Открытый ключ:

Алгоритм открытого ключа:

Название:

GOST R 34.10-2001

Идентификатор:

1.2.643.2.2.19

Параметры:

```
30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03 02 02 1e 01
```

Значение:

```
0440 CE4A D06B 8B97 F54D 1FC4 8FB8 1FA1 F460
5445 FC7E 77D7 6D96 D78B C67B 6833 AC24 C76F
2C87 56EE E076 B0EA 9179 8781 01DB EC79 3FC9
B7F0 9117 CB52 7ECF F80D E3F2
```

Расширения X.509

1. Расширение 2.5.29.15

Название:

Key Usage

Значение:

```
Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
(86)
```

2. Расширение 2.5.29.19 (критическое)

Название:

Basic Constraints

Значение:

```
Subject Type=CA
Path Length Constraint=None
```

3. Расширение 2.5.29.14

Название:

Subject Key Identifier

Значение:

```
12 d6 28 dc d5 c2 dd 27 db 30 f8 84 b5 84 72 12 01 84 00 a1
```

4. Расширение 2.5.29.31

Название:

CRL Distribution Points

Значение:

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://ca.y-center.ru/crl.crl
```

5. Расширение 1.3.6.1.4.1.311.21.1

Название:

CA Version

Значение:

```
V5.5
```

6. Расширение 1.3.6.1.4.1.311.21.2

Название:

Previous CA Certificate Hash

Значение:

```
60 5a b1 2d a1 2b 7b 12 f0 bc e8 f9 6b 56 09 c4 f3 80 2b 21
```

ЭЦП:

Алгоритм ЭЦП:

Название:

GOST R 34.11/34.10-2001

Идентификатор:

1.2.643.2.2.3

Параметры:

```
05 00
```

Значение:

```
4E67 1BA3 4218 13A6 1E4B E3DD 8EE9 3235 0E3F
6874 FF9A 7DC0 DDCD 280B 14BC 6700 8CED 37FB
AF64 42EB 3022 6312 79B1 8877 A71B 96DD DD0D
8762 12DE 8BFC 24B9 2887
```

Описание отчета о подтверждении подлинности ЭЦП электронного документа

Ниже приведен пример отчета о подтверждении подлинности ЭЦП электронного документа.

Комментарии к отчету отмечены курсивом и красным цветом.

Общий результат подтверждения подлинности ЭЦП:

Результат подтверждения подлинности ЭЦП - подлинность ПОДТВЕРЖДЕНА

Краткая форма отчета:

Краткая информация по каждой из ЭЦП в документе:

Информация по первой ЭЦП:

ЭЦП 1: ВЕРНА

Информация о статусе сертификата:

Статус сертификата подписи - ДЕЙСТВИТЕЛЕН

TestGostNet, Sharpei, CryptoPro, RU :

```
Действителен
```

test-ca, cp, ru :

```
Действителен
```

Информация по следующей ЭЦП:

ЭЦП 2: ВЕРНА

Информация о статусе сертификата:

Статус сертификата подписи - ДЕЙСТВИТЕЛЕН

TestEncryptNet, Sharpei, CryptoPro, RU :

Действителен

test-ca, cp, ru :

Действителен

Полная форма отчета:

Отчет о подтверждении подлинности ЭЦП

Время создания отчета: 28 января 2011 14:14:31 (28 января 2011 11:14:31)

Время, на которое проводилась проверка: 28 января 2011 14:14:26 (28 января 2011 11:14:26)

Проверен файл: размер (в байтах) 2456

Размер обработанного криптографического сообщения (в байтах): 2456

Количество проверенных ЭЦП: 2

Информация по каждой из ЭЦП в документе:

Информация по первой ЭЦП:

Результат подтверждения подлинности ЭЦП номер 1

ЭЦП - ВЕРНА

Время создания ЭЦП: не определено

В проверенном атрибуте подписи (1.2.840.113549.1.9.5) указано время подписания 12 января 2011 14:19:21

Время проверки ЭЦП: 28 января 2011 11:14:26

Информация об ЭЦП:

Алгортим хэширования:

Название:

ГОСТ Р 34.11-94

Идентификатор:

1.2.643.2.2.9

Алгортим открытого ключа:

Название:

ГОСТ Р 34.10-2001

Идентификатор:

1.2.643.2.2.19

Значение:

```
8F5D D050 009C A602 66F5 C0D1 3340 9909
1D9B 0BEA B768 FD92 F13E 18FF 1B40 55C3
707C E813 4668 8CFF 1CA0 4C3F 2380 F0FF
DB50 7E22 59FC C938 C0E8 4E2E 73A3 3297
```

Информация о сертификате, использованном для подтверждения подлинности ЭЦП:

Серийный номер: 20C1 9812 0000 0046 1B31

Владелец сертификата: TestGostNet, Sharpei, CryptoPro, RU

ЭЦП уполномоченных лиц удостоверяющих центров в цепочке сертификатов - ВЕРНА

Статус сертификата подписи - ДЕЙСТВИТЕЛЕН

Информация и штампах времени в составе подписи:

Количество штампов времени на подпись: 0

Информация о сохраненных результатах онлай проверки статуса сертификата в составе подписи:

Количество OCSP-ответов в подписи: 0

Результат установления статуса цепочки сертификатов

Владелец сертификата: TestGostNet, Sharpei, CryptoPro, RU

Уполномоченное лицо: test-ca, cp, ru

Серийный номер: 20C1 9812 0000 0046 1B31

Результат установления статуса сертификата

Действителен

Информация о приостановлении действия или аннулировании сертификата (с использованием списка отозванных сертификатов):

Найдено СОС: 1

Результат проверки СОС номер 1

Уполномоченное лицо: test-ca, cp, ru

Идентификатор ключа:

Значение:

```
9E03 F0B8 9CFC 60DC 8A18 1EE8 0000 0000
0000 0000
```

Номер СОС: 99

Действителен с:

27 января 2011 00:03:56

Действителен по:

04 февраля 2011 01:23:56

Статус СОС: Действителен

Информация о сертификате из списка отзыва:

```
Действителен
```

Информация о приостановлении действия или аннулировании сертификата (с использованием онлайн проверки статуса):

Найдено статусов в OCSP-ответах: 0

Владелец сертификата: test-ca, cp, ru

Уполномоченное лицо: test-ca, cp, ru

Серийный номер: 2F3B 739C F868 9CBD 44F3 B321 8251 664C

Результат установления статуса сертификата

```
Действителен
```

Информация по каждому из сертификатов, использованному при подтверждении подлинности:

Сертификаты, использованные при подтверждении подлинности ЭЦП

Информация по сертификату:

Сертификат X.509:

Сведения о сертификате:

Этот сертификат:

Подтверждает удаленному компьютеру идентификацию вашего компьютера

Кому выдан:

TestGostNet

Кем выдан:

test-ca

Действителен с 14 декабря 2010 г. 1:06:34 UTC по 14 декабря 2020 г. 7:46:34 UTC

Версия: 3 (0x2)

Серийный номер:

`20C1 9812 0000 0046 1B31`

Уполномоченное лицо:

CN = test-ca

DC = cp

DC = ru

Срок действия:

Действителен с:

14 декабря 2010 г. 1:06:34 UTC

Действителен по:

14 декабря 2020 г. 7:46:34 UTC

Владелец сертификата:

CN = TestGostNet

OU = Sharpei

O = CryptoPro

C = RU

Открытый ключ:

Алгоритм открытого ключа:

Название:

ГОСТ Р 34.10-2001

Идентификатор:

1.2.643.2.2.19

Параметры:

```
30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
```

Значение:

```
0440 9E72 508C 7902 AB92 D7F3 39E7 5364
67A6 5E41 12D4 CF6F 8B2F 33F9 516E 2C79
53BA B6BD CE42 78C5 B367 04DE 34DC 8BDB
B082 D34F 8E98 6375 C401 793E 6AA2 170B
E3C2
```

Расширения X.509

1. Расширение 2.5.29.37

Название:

Улучшенный ключ

Значение:

```
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
```

2. Расширение 2.5.29.15 (критическое)

Название:

Использование ключа

Значение:

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

3. Расширение 2.5.29.14

Название:

Идентификатор ключа субъекта

Значение:

```
e8 34 d1 f0 3f 79 fe be bf 4c 23 0d 20 c9 c9 09 80 e9 77 3d
```

4. Расширение 2.5.29.35

Название:

Идентификатор ключа центра сертификатов

Значение:

```
Идентификатор ключа=9e 03 f0 b8 9c fc 60 dc 8a 18 1e e8 00 df a8 5b 32 cd 73
76
```

5. Расширение 2.5.29.31

Название:

Точки распространения списков отзыва (CRL)

Значение:

```
[1]Точка распределения списка отзыва (CRL)
     Имя точки распространения:
          Полное имя:
               URL=http://vm-test-ca.cp.ru/CertEnroll/test-ca.crl
```

6. Расширение 1.3.6.1.5.5.7.1.1

Название:

Доступ к информации о центрах сертификации

Значение:

```
[1]Доступ к сведениям центра сертификации
     Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)
     Дополнительное имя:
          URL=http://vm-test-ca.cp.ru/CertEnroll/vm-test-ca.cp.ru_test-ca.crt
[2]Доступ к сведениям центра сертификации
     Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)
     Дополнительное имя:
          URL=file://\\vm-test-ca.cp.ru\CertEnroll\vm-test-ca.cp.ru_test-
ca.crt
```

ЭЦП:

Алгоритм ЭЦП:

Название:

ГОСТ Р 34.11/34.10-2001

Идентификатор:

1.2.643.2.2.3

Значение:

```
31CC 9E14 3543 65EE 2353 3639 ABFB 8A82
65A2 F2D2 F4D1 8570 CA16 2BBF D605 1EB2
8C4A C030 C103 A449 C0A4 928C E6CE 337D
DF23 CFC4 24F4 D50D FC77 074F 0BBF 70FD
```

Информация по сертификату:

Сертификат X.509:

Сведения о сертификате:

Кому выдан:

test-ca

Кем выдан:

test-ca

Действителен с 19 мая 2008 г. 12:05:34 UTC по 19 мая 2038 г. 12:14:58 UTC

Версия: 3 (0x2)

Серийный номер:

```
2F3B 739C F868 9CBD 44F3 B321 8251 664C
```

Уполномоченное лицо:

CN = test-ca

DC = cp

DC = ru

Срок действия:

Действителен с:

19 мая 2008 г. 12:05:34 UTC

Действителен по:

19 мая 2038 г. 12:14:58 UTC

Владелец сертификата:

CN = test-ca

DC = cp

DC = ru

Открытый ключ:

Алгоритм открытого ключа:

Название:

ГОСТ Р 34.10-2001

Идентификатор:

1.2.643.2.2.19

Параметры:

```
30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03 02 02 1e 01
```

Значение:

```
0440 330D 0311 1D7C 2630 6E65 8885 DFC2
2122 EE83 E901 D576 AC6D EFFF 635C 8B7B
ACB4 FC8C 1AE9 8626 2CA2 CA7C 5B62 32AC
B735 22AC C8F3 54AE A5BE 2806 0E0D 20A3
B289
```

Расширения X.509

1. Расширение 1.3.6.1.4.1.311.20.2

Название:

Имя шаблона сертификата

Значение:

```
CA
```

2. Расширение 2.5.29.15

Название:

Использование ключа

Значение:

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

3. Расширение 2.5.29.19 (критическое)

Название:

Основные ограничения

Значение:

```
Тип субъекта=ЦС
Ограничение на длину пути=Отсутствует
```

4. Расширение 2.5.29.14

Название:

Идентификатор ключа субъекта

Значение:

```
9e 03 f0 b8 9c fc 60 dc 8a 18 1e e8 00 df a8 5b 32 cd 73 76
```

5. Расширение 2.5.29.31

Название:

Точки распространения списков отзыва (CRL)

Значение:

```
[1]Точка распределения списка отзыва (CRL)
     Имя точки распространения:
          Полное имя:
               URL=http://vm-test-ca.cp.ru/CertEnroll/test-ca.crl
```

6. Расширение 1.3.6.1.4.1.311.21.1

Название:

Версия ЦС

Значение:

```
V0.0
```

ЭЦП:

Алгоритм ЭЦП:

Название:

ГОСТ Р 34.11/34.10-2001

Идентификатор:

1.2.643.2.2.3

Значение:

```
1B6B 9C06 5A92 510C ED56 BE24 E827 BFF4
6B00 76A5 909A 44B3 67D4 4963 A7CD A223
5B6D 07C0 434A AB6B 0BD3 2DF4 3A08 69E3
B01F 085E 4432 F9C4 2025 7677 8533 B797
```

Информация по следующей ЭЦП:

Результат подтверждения подлинности ЭЦП номер 2

ЭЦП - ВЕРНА

Время создания ЭЦП: не определено

В проверенном атрибуте подписи (1.2.840.113549.1.9.5) указано время подписания 12 января 2011 14:19:55

Время проверки ЭЦП: 28 января 2011 11:14:26

Информация об ЭЦП:

Алгортим хэширования:

Название:

ГОСТ Р 34.11-94

Идентификатор:

1.2.643.2.2.9

Алгортим открытого ключа:

Название:

ГОСТ Р 34.10-2001

Идентификатор:

1.2.643.2.2.19

Значение:

```
4391 7732 2E06 3F01 E709 B808 9495 BF02
F14E 88E6 7134 FB14 FCD5 242C DEA2 E06C
4DA9 7D1F F8FE 2BF7 EA6F 9586 0446 B135
C428 6479 E0AC 1196 D4A2 3A0F 5450 36D5
```

Серийный номер: 20C1 C23F 0000 0046 1B32

Владелец сертификата: TestEncryptNet, Sharpei, CryptoPro, RU

ЭЦП уполномоченных лиц удостоверяющих центров в цепочке сертификатов - ВЕРНА

Статус сертификата подписи - ДЕЙСТВИТЕЛЕН

Количество штампов времени на подпись: 0

Количество OCSP-ответов в подписи: 0

Результат установления статуса цепочки сертификатов

Владелец сертификата: TestEncryptNet, Sharpei, CryptoPro, RU

Уполномоченное лицо: test-ca, cp, ru

Серийный номер: 20C1 C23F 0000 0046 1B32

Результат установления статуса сертификата

```
Действителен
```

Найдено СОС: 1

Результат проверки СОС номер 1

Уполномоченное лицо: test-ca, cp, ru

Идентификатор ключа:

Значение:

```
9E03 F0B8 9CFC 60DC 8A18 1EE8 0000 0000
0000 0000
```

Номер СОС: 99

Действителен с:

27 января 2011 00:03:56

Действителен по:

04 февраля 2011 01:23:56

Статус СОС: Действителен

Информация о сертификате из списка отзыва:

Действителен

Найдено статусов в OCSP-ответах: 0

Владелец сертификата: test-ca, cp, ru

Уполномоченное лицо: test-ca, cp, ru

Серийный номер: 2F3B 739C F868 9CBD 44F3 B321 8251 664C

Результат установления статуса сертификата

Действителен

Сертификаты, использованные при подтверждении подлинности ЭЦП

Сертификат X.509:

Сведения о сертификате:

Этот сертификат:

Подтверждает удаленному компьютеру идентификацию вашего компьютера

Кому выдан:

TestEncryptNet

Кем выдан:

test-ca

Действителен с 14 декабря 2010 г. 1:06:45 UTC по 14 декабря 2020 г. 7:46:45 UTC

Версия: 3 (0x2)

Серийный номер:

20C1 C23F 0000 0046 1B32

Уполномоченное лицо:

CN = test-ca

DC = cp

DC = ru

Срок действия:

Действителен с:

14 декабря 2010 г. 1:06:45 UTC

Действителен по:

14 декабря 2020 г. 7:46:45 UTC

Владелец сертификата:

CN = TestEncryptNet

OU = Sharpei

O = CryptoPro

C = RU

Открытый ключ:

Алгоритм открытого ключа:

Название:

ГОСТ Р 34.10-2001

Идентификатор:

1.2.643.2.2.19

Параметры:

```
30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
```

Значение:

```
0440 9704 BB6B 1DC4 3F7E 7678 93DB 1FBB
1828 2994 4076 99B6 D42D 9CB5 FE4A A9C6
560C A41B 7965 B0C4 FF4B 4E6C 4750 D6AB
4C9D 3E24 FCA9 2E07 F6C4 A421 D249 B024
3499
```

Расширения X.509

1. Расширение 2.5.29.37

Название:

Улучшенный ключ

Значение:

```
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
```

2. Расширение 2.5.29.15 (критическое)

Название:

Использование ключа

Значение:

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

3. Расширение 2.5.29.14

Название:

Идентификатор ключа субъекта

Значение:

```
e1 43 5e c4 fe 60 8c ed d6 76 3d eb 70 47 66 a0 e1 c0 68 0a
```

4. Расширение 2.5.29.35

Название:

Идентификатор ключа центра сертификатов

Значение:

```
Идентификатор ключа=9e 03 f0 b8 9c fc 60 dc 8a 18 1e e8 00 df a8 5b 32 cd 73
76
```

5. Расширение 2.5.29.31

Название:

Точки распространения списков отзыва (CRL)

Значение:

```
[1]Точка распределения списка отзыва (CRL)
     Имя точки распространения:
          Полное имя:
               URL=http://vm-test-ca.cp.ru/CertEnroll/test-ca.crl
```

6. Расширение 1.3.6.1.5.5.7.1.1

Название:

Доступ к информации о центрах сертификации

Значение:

```
[1]Доступ к сведениям центра сертификации
     Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)
     Дополнительное имя:
          URL=http://vm-test-ca.cp.ru/CertEnroll/vm-test-ca.cp.ru_test-ca.crt
[2]Доступ к сведениям центра сертификации
     Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)
     Дополнительное имя:
          URL=file://\\vm-test-ca.cp.ru\CertEnroll\vm-test-ca.cp.ru_test-
ca.crt
```

ЭЦП:

Алгоритм ЭЦП:

Название:

ГОСТ Р 34.11/34.10-2001

Идентификатор:

1.2.643.2.2.3

Значение:

```
98EF 0377 DEF9 20D0 FFD9 CEFE 584E E569
29CF 242B D7EC F53B B273 5232 E933 BBE6
076F 8475 0DF5 693A 0108 0BA6 4898 5EC0
096A 376F 7E51 0DAF 8EAC 803D C5C0 9607
```

Сертификат X.509:

Сведения о сертификате:

Кому выдан:

test-ca

Кем выдан:

test-ca

Действителен с 19 мая 2008 г. 12:05:34 UTC по 19 мая 2038 г. 12:14:58 UTC

Версия: 3 (0x2)

Серийный номер:

```
2F3B 739C F868 9CBD 44F3 B321 8251 664C
```

Уполномоченное лицо:

CN = test-ca

DC = cp

DC = ru

Срок действия:

Действителен с:

19 мая 2008 г. 12:05:34 UTC

Действителен по:

19 мая 2038 г. 12:14:58 UTC

Владелец сертификата:

CN = test-ca

DC = cp

DC = ru

Открытый ключ:

Алгоритм открытого ключа:

Название:

ГОСТ Р 34.10-2001

Идентификатор:

1.2.643.2.2.19

Параметры:

```
30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03 02 02 1e 01
```

Значение:

```
0440 330D 0311 1D7C 2630 6E65 8885 DFC2
2122 EE83 E901 D576 AC6D EFFF 635C 8B7B
ACB4 FC8C 1AE9 8626 2CA2 CA7C 5B62 32AC
B735 22AC C8F3 54AE A5BE 2806 0E0D 20A3
B289
```

Расширения X.509

1. Расширение 1.3.6.1.4.1.311.20.2

Название:

Имя шаблона сертификата

Значение:

```
CA
```

2. Расширение 2.5.29.15

Название:

Использование ключа

Значение:

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

3. Расширение 2.5.29.19 (критическое)

Название:

Основные ограничения

Значение:

```
Тип субъекта=ЦС
Ограничение на длину пути=Отсутствует
```

4. Расширение 2.5.29.14

Название:

Идентификатор ключа субъекта

Значение:

```
9e 03 f0 b8 9c fc 60 dc 8a 18 1e e8 00 df a8 5b 32 cd 73 76
```

5. Расширение 2.5.29.31

Название:

Точки распространения списков отзыва (CRL)

Значение:

```
[1]Точка распределения списка отзыва (CRL)
     Имя точки распространения:
          Полное имя:
```

URL=http://vm-test-ca.cp.ru/CertEnroll/test-ca.crl

6. Расширение 1.3.6.1.4.1.311.21.1

Название:

Версия ЦС

Значение:

V0.0

ЭЦП:

Алгоритм ЭЦП:

Название:

ГОСТ Р 34.11/34.10-2001

Идентификатор:

1.2.643.2.2.3

Значение:

```
1B6B 9C06 5A92 510C ED56 BE24 E827 BFF4
6B00 76A5 909A 44B3 67D4 4963 A7CD A223
5B6D 07C0 434A AB6B 0BD3 2DF4 3A08 69E3
B01F 085E 4432 F9C4 2025 7677 8533 B797
```