# Утилита для работы с сертификатами на токене PKCS#11
# Руководство пользователя

ООО "ЛИССИ-Софт"

7 мая 2015 г.

# Оглавление

# 1 Введение

Утилита p11cert является средством для выполнения вспомогательных операций с сертификатами на токене PKCS#11 [5]. Утилита обеспечивает поддержку российских криптографических алгоритмов в соответствии со спецификациями, выработанными Техническим комитетом по стандартизации (ТК 26) "Криптографическая защита информации" [2, 3], включая алгоритмы ГОСТ Р34.10-2012, ГОСТ Р34.11-2012, а также сопутствующие алгоритмы и параметры, определенные руководящими документами ТК 26.

В то же время, утилита p11cert не зависит от конкретной библиотеки и может работать с любой библиотекой PKCS#11 и, следовательно, с любыми токенами, поддерживающими данный интерфейс.

## 1.1 Системные требования

Утилита p11cert реализована кросс-платформенным образом и работает в режиме командной строки, так что она, в принципе, может быть портирована в любую операционную систему, где поддерживается язык Си. Текущая версия работает в операционных системах Windows, Linux и Mac OS X на 32-х и 64-х разрядных платформах.

# 2 Основные сведения

## 2.1 Состав и структура

Утилита p11cert входит в состав проекта p11conf. В проект p11conf входят:

- Утилита конфигурирования токена p11conf
- Утилита конфигурирования токена p11cert
- Руководства пользователя к утилитам

Выполняемый файл утилиты p11cert в Windows называется p11cert.exe, а в Linux и Mac OS X – просто p11cert.

## 2.2 Установка

Утилита p11cert устанавливается инсталлятором p11conf в целевую папку вместе с утилитой p11conf.

Важное замечание. На целевой платформе нужно обеспечить прикладным программам возможность найти утилиту по имени путем добавления полного пути к содержащей ее папке к значению переменной среды PATH.

Документация для p11cert скачивается отдельно с сайта "ЛИССИ-Софт"[1].

## 2.3 Лицензирование

В отличие от свободно распространяемой утилиты p11conf, утилита p11cert использует лицензионные ресурсы и требует лицензирования на сайте производителя – ООО "ЛИССИ-Софт"[1]. Если у пользователя уже имеется лицензия для продукта LCSSL, то отдельное лицензирование для p11cert не требуется. Если лицензии для LCSSL нет, то для продукта P11CERT нужна отдельная лицензия.

## 2.4 Примеры использования

Утилита предоставляет возможности, о которых сообщается при запуске команды `p11cert -h`. К ним относятся импорт и экспорт сертификатов, просмотр их содержимого и др. Следующие примеры показывают опции утилиты p11cert и их использование.

```
>p11cert -h
usage:  p11cert -p11 <PKCS#11 library path> [options]
options:
        -help           - display usage
        -p11info        - display PKCS#11 library info
        -slotlist       - display slots info
        -slot <slot ID> - set token slot ID
                          (first with token present by default)
        -tokeninfo      - display token info
        -certlist       - enumerate all certificates
        -label <label>  - token object label
        -print          - print certificate to standard output
        -pkeyfind       - search for certificate private key
        -attributes     - dump all certificate attributes
        -remove         - remove certificate from the token
        -outfile        - export certificate to output file path
        -outform        - output file format (pem|der)
                                        (pem by default)
        -infile         - import from file path
        -inform         - import file format (pem|der|pfx|p12
                                        (pem by default).
            NB: Import from the pfx(p12) format creates
                private key, public key and certificate
                objects on the token with the same label.
                Import from the pem/der format creates
                the certificate token object only.
Copyright(C) LISSI-Soft Ltd (http://soft.lissi.ru) 2015
```

Единственным обязательным параметром при вызове утилиты является путь к библиотеке PKCS#11. Если не указывать других опций, то утилита выдает только информацию о библиотеке. Данная информация выдается также с опцией -p11info.

Список слотов с токенами выдается, если задана опция -slotlist. Для каждого токена выдается информация о слоте, включая его идентификатор, и о текене, подключенном к слоту.

Обычно пользователь работает с одним-единственным слотом, идентификатор которого задается в опции -slot. Например, для получения информации о конкретном токене нужно задать опции -slot и -tokeninfo.

Далее приводятся некоторые примеры использования утилиты с библиотекой ls11sw2012.dll в среде Windows. В этой среде допускается использование с опцией -p11 имени библиотеки без расширения, если путь к папке, содержащей библиотеку, конфигурирован соответствующим образом в переменной среды PATH. В Linux библиотека называется libls11sw2012.so, в Mac OS X – libls11sw2012.dylib. В этих операционных системах нужно указывать имя библиотеки с префиксом lib и с расширением, а путь к папке, содержащей библиотеку, должен быть прописан в пе-

ременной среды LD_LIBRARY_PATH. Впрочем, с флагом -p11 можно использовать и полный путь к файлу библиотеки.

### 2.4.1 Получение информации о библиотеке

```
> p11cert -p11 ls11sw2012
PKCS#11 Info
        Version 2.30
        Manufacturer: LISSI-Soft
        Flags: 0x0
        Library Description: ls11sw2012 PKCS#11 library
        Library Version 5.0
OK
```

### 2.4.2 Получение информации о слотах и токенах

```
>p11cert -p11 ls11sw2012 -slotlist
Slot with ID 0 Info
        Description: LS11SW Slot 0
        Manufacturer: LISSI-Soft Ltd
        Flags: 0x1 ( TOKEN_PRESENT )
        Hardware Version: 1.0
        Firmware Version: 1.0
Token #0 Info:
        Label: vblazhnov
        Manufacturer: LISSI-Soft Ltd
        Model: LS11SW
        Serial Number: 398C6DCCF325CA1E
        Flags: 0x40D ( RNG|LOGIN_REQUIRED|USER_PIN_INITIALIZED|TOKEN_INITIALIZED )
        Sessions: 1/256
        R/W Sessions: 1/256
        PIN Length: 4-32
        Public Memory: 0xFFFFFFFF/0xFFFFFFFF
        Private Memory: 0xFFFFFFFF/0xFFFFFFFF
        Hardware Version: 1.0
        Firmware Version: 1.0
        Time: 11:22:29
OK
```

### 2.4.3 Получение информации о токене

```
>p11cert -p11 ls11sw2012 -slot 0 -tokeninfo
Token #0 Info:
        Label: vblazhnov
        Manufacturer: LISSI-Soft Ltd
```

```
        Model: LS11SW
        Serial Number: 398C6DCCF325CA1E
        Flags: 0x40D ( RNG|LOGIN_REQUIRED|USER_PIN_INITIALIZED|TOKEN_INITIALIZED )
        Sessions: 1/256
        R/W Sessions: 1/256
        PIN Length: 4-32
        Public Memory: 0xFFFFFFFF/0xFFFFFFFF
        Private Memory: 0xFFFFFFFF/0xFFFFFFFF
        Hardware Version: 1.0
        Firmware Version: 1.0
        Time: 11:23:48
OK
```

### 2.4.4 Получение списка сертификатов

Выдается список сертификатов на токене.

```
>p11cert -p11 ls11sw2012 -slot 0 -certlist
Certificate objects:
1: label: 'pki'
OK
```

Метка сертификата на токене, выдаваемая в данном списке, в дальнейшем служит для идентификации конкретного сертификата.

### 2.4.5 Поиск закрытого ключа

С опцией -pkeyfind производится поиск на токене закрытого ключа для данного сертификата по значению атрибута `CKA_ID`, которым обычно связываются объекты ключевой пары на токене. Для выполнения операции с закрытыми ключами утилита запрашивает PIN пользователя:

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -pkeyfind
Enter user PIN:
Certificate label: 'pki'
Private key found, label: 'pki'
OK
```

### 2.4.6 Выдача содержимого сертификата

Выдается содержимое всех полей сертификата в стандартный вывод.

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -print
Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number: 21731 (0x54e3)
    Signature Algorithm: GOST R 34.11-94 with GOST R 34.10-2001
        Issuer: INN=005054090835/OGRN=1095018003420, L=г.Юбилейный,
        ST=50 Московская область, C=RU, O=ООО ЛИССИ-Софт,
        OU=Тестовый УЦ, CN=ООО ЛИССИ-Софт/emailAddress=info@lissi.ru
        Validity
            Not Before: Nov 19 14:27:06 2014 GMT
            Not After : Nov 19 14:27:06 2015 GMT
        Subject: O=ЛИССИ-Софт/street=Ленинская 4, помещение 7, L=Королев,
        ST=50  Московская область   , C=RU, GN=Валерий Юрьевич,
        SN=Блажнов, CN=Блажнов В.Ю.
        /emailAddress=vblazhnov@lissi-crypto.ru/serialNumber=21731
        Subject Public Key Info:
            Public Key Algorithm: GOST R 34.10-2001
                Public key:
0xbb, 0xcf, 0x7d, 0xb4, 0x3d, 0xbd, 0x7f, 0x09,
0x11, 0x60, 0xc9, 0xc3, 0x17, 0x16, 0xe4, 0xfe,
0xdd, 0xf3, 0x02, 0x10, 0xdf, 0x77, 0xf1, 0xe1,
0x3c, 0x22, 0x25, 0x6b, 0x1f, 0xeb, 0x07, 0x14,
0xa0, 0x45, 0x99, 0x3d, 0x20, 0x44, 0x44, 0x5d,
0x63, 0xe3, 0x19, 0x8c, 0xc5, 0x65, 0x14, 0xe3,
0x3e, 0x03, 0xe0, 0x2a, 0x91, 0x75, 0x1b, 0x0e,
0x12, 0x93, 0x7f, 0xdb, 0xcb, 0x72, 0x98, 0xd1,

                Parameter set: id-GostR3410-2001-CryptoPro-XchA-ParamSet
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection,
                Microsoft Smartcardlogin
            X509v3 Subject Key Identifier:
                BB:AB:03:54:AF:26:AE:51:63:A1:5E:12:B6:A3:6D:D5:D8:47:A3:B5
            X509v3 Authority Key Identifier:
                keyid:
                A2:B8:8C:07:47:A0:1F:88:DD:14:37:6A:13:65:69:3C:DE:28:B4:CB
                DirName:/INN=005054090835/OGRN=1095018003420/L=г.Юбилейный
                /ST=50 Московская область/C=RU/O=ООО ЛИССИ-Софт/
                OU=Тестовый УЦ
                serial:00
```

```
            X509v3 Subject Alternative Name:
                email:vblazhnov@lissi-crypto.ru
            X509v3 Issuer Alternative Name:
                email:info@lissi.ru
            Issuer Sign Tool:
                ПБЗИ «СКЗИ «ЛИРССЛ»
                Программно аппаратный комплекс «ЛИССИ-УЦ»
                СФ/111-1979 от 01.02.2013
                СФ/121-1870 от 26.06.2012

            Subject Sign Tool:
                ПБЗИ «СКЗИ «ЛИРССЛ»
            X509v3 Certificate Policies:
                Policy: KC1 Class Sign Tool
                Policy: KC2 Class Sign Tool

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://ca.soft.lissi.ru/pub/crl/cacrl.crl

    Signature Algorithm: GOST R 34.11-94 with GOST R 34.10-2001
         5a:dc:fb:e4:55:ed:c8:a6:1e:f2:4b:e8:45:cd:2b:32:30:ac:
         e4:4a:56:23:8c:00:ca:c8:83:d1:d0:f3:f0:0c:77:53:d6:c0:
         2e:72:c7:f4:79:10:4c:ba:4b:72:e2:08:34:37:8a:f7:78:64:
         86:a9:10:fc:95:de:7d:63:e8:16
OK
```

При необходимости, вывод утилиты может быть перенаправлен в файл добавлением в конце командной строки `> имя-файла`:

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -print > pki.txt
```

В системе Windows экран командной строки по умолчанию работает в кодировке 866, а многие поля сертификата используют кодировку UTF-8. Для правильного визуального отображения полей с русскими буквами в окне следует установить шрифт Lucida Console в свойствах окна и затем командой chcp переключить кодировку на UTF-8 (65001) перед командой выдачи содержимого сертификата:

```
>chcp 65001 & p11cert -p11 ls11sw2012 -slot 0 -label pki -print
```

Заметим, что в окне популярной программы far по умолчанию уже установлен шрифт Lucida Console.

### 2.4.7 Удаление сертификата

Удаление сертификата с токена производится с опцией -remove. Поскольку обычно требуется логин для любых изменений на токене, то утилита запросит PIN пользователя.

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki2 -remove
Enter token user PIN:
Certificate object 'pki2' removed from the token
OK
```

### 2.4.8 Дамп атрибутов объекта сертификата

С опцией -attributes выдается шестнадцатеричный дамп значений всех атрибутов объекта сертификата на токене:

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -attributes
label: 'pki'
==================================
Object handle: 0x1
----------------------------------
CKA_CLASS
0x01, 0x00, 0x00, 0x00,

CKA_TOKEN
0x01,

CKA_PRIVATE
0x00,

CKA_LABEL
0x70, 0x6b, 0x69, 0x00,

CKA_VALUE
0x30, 0x82, 0x06, 0xb9, 0x30, 0x82, 0x06, 0x66,
0xa0, 0x03, 0x02, 0x01, 0x02, 0x02, 0x02, 0x54,
0xe3, 0x30, 0x0a, 0x06, 0x06, 0x2a, 0x85, 0x03,
0x02, 0x02, 0x03, 0x05, 0x00, 0x30, 0x82, 0x01,
0x1c, 0x31, 0x1a, 0x30, 0x18, 0x06, 0x08, 0x2a,
0x85, 0x03, 0x03, 0x81, 0x03, 0x01, 0x01, 0x12,
0x0c, 0x30, 0x30, 0x35, 0x30, 0x35, 0x34, 0x30,
0x39, 0x30, 0x38, 0x33, 0x35, 0x31, 0x18, 0x30,
0x16, 0x06, 0x05, 0x2a, 0x85, 0x03, 0x64, 0x01,
0x12, 0x0d, 0x31, 0x30, 0x39, 0x35, 0x30, 0x31,
0x38, 0x30, 0x30, 0x33, 0x34, 0x32, 0x30, 0x31,
```

```
0x1e, 0x30, 0x1c, 0x06, 0x03, 0x55, 0x04, 0x07,
0x0c, 0x15, 0xd0, 0xb3, 0x2e, 0xd0, 0xae, 0xd0,
0xb1, 0xd0, 0xb8, 0xd0, 0xbb, 0xd0, 0xb5, 0xd0,
0xb9, 0xd0, 0xbd, 0xd1, 0x8b, 0xd0, 0xb9, 0x31,
0x2f, 0x30, 0x2d, 0x06, 0x03, 0x55, 0x04, 0x08,
0x0c, 0x26, 0x35, 0x30, 0x20, 0xd0, 0x9c, 0xd0,
0xbe, 0xd1, 0x81, 0xd0, 0xba, 0xd0, 0xbe, 0xd0,
0xb2, 0xd1, 0x81, 0xd0, 0xba, 0xd0, 0xb0, 0xd1,
0x8f, 0x20, 0xd0, 0xbe, 0xd0, 0xb1, 0xd0, 0xbb,
0xd0, 0xb0, 0xd1, 0x81, 0xd1, 0x82, 0xd1, 0x8c,
0x31, 0x0b, 0x30, 0x09, 0x06, 0x03, 0x55, 0x04,
0x06, 0x13, 0x02, 0x52, 0x55, 0x31, 0x23, 0x30,
0x21, 0x06, 0x03, 0x55, 0x04, 0x0a, 0x0c, 0x1a,
0xd0, 0x9e, 0xd0, 0x9e, 0xd0, 0x9e, 0x20, 0xd0,
0x9b, 0xd0, 0x98, 0xd0, 0xa1, 0xd0, 0xa1, 0xd0,
0x98, 0x2d, 0xd0, 0xa1, 0xd0, 0xbe, 0xd1, 0x84,
0xd1, 0x82, 0x31, 0x1e, 0x30, 0x1c, 0x06, 0x03,
0x55, 0x04, 0x0b, 0x0c, 0x15, 0xd0, 0xa2, 0xd0,
0xb5, 0xd1, 0x81, 0xd1, 0x82, 0xd0, 0xbe, 0xd0,
0xb2, 0xd1, 0x8b, 0xd0, 0xb9, 0x20, 0xd0, 0xa3,
0xd0, 0xa6, 0x31, 0x23, 0x30, 0x21, 0x06, 0x03,
0x55, 0x04, 0x03, 0x0c, 0x1a, 0xd0, 0x9e, 0xd0,
0x9e, 0xd0, 0x9e, 0x20, 0xd0, 0x9b, 0xd0, 0x98,
0xd0, 0xa1, 0xd0, 0xa1, 0xd0, 0x98, 0x2d, 0xd0,
0xa1, 0xd0, 0xbe, 0xd1, 0x84, 0xd1, 0x82, 0x31,
0x1c, 0x30, 0x1a, 0x06, 0x09, 0x2a, 0x86, 0x48,
0x86, 0xf7, 0x0d, 0x01, 0x09, 0x01, 0x16, 0x0d,
0x69, 0x6e, 0x66, 0x6f, 0x40, 0x6c, 0x69, 0x73,
0x73, 0x69, 0x2e, 0x72, 0x75, 0x30, 0x1e, 0x17,
0x0d, 0x31, 0x34, 0x31, 0x31, 0x31, 0x39, 0x31,
0x34, 0x32, 0x37, 0x30, 0x36, 0x5a, 0x17, 0x0d,
0x31, 0x35, 0x31, 0x31, 0x31, 0x39, 0x31, 0x34,
0x32, 0x37, 0x30, 0x36, 0x5a, 0x30, 0x82, 0x01,
0x5c, 0x31, 0x1d, 0x30, 0x1b, 0x06, 0x03, 0x55,
0x04, 0x0a, 0x1e, 0x14, 0x04, 0x1b, 0x04, 0x18,
0x04, 0x21, 0x04, 0x21, 0x04, 0x18, 0x00, 0x2d,
0x04, 0x21, 0x04, 0x3e, 0x04, 0x44, 0x04, 0x42,
0x31, 0x39, 0x30, 0x37, 0x06, 0x03, 0x55, 0x04,
0x09, 0x1e, 0x30, 0x04, 0x1b, 0x04, 0x35, 0x04,
0x3d, 0x04, 0x38, 0x04, 0x3d, 0x04, 0x41, 0x04,
0x3a, 0x04, 0x30, 0x04, 0x4f, 0x00, 0x20, 0x00,
0x34, 0x00, 0x2c, 0x00, 0x20, 0x04, 0x3f, 0x04,
0x3e, 0x04, 0x3c, 0x04, 0x35, 0x04, 0x49, 0x04,
0x35, 0x04, 0x3d, 0x04, 0x38, 0x04, 0x35, 0x00,
```

```
0x20, 0x00, 0x37, 0x31, 0x17, 0x30, 0x15, 0x06,
0x03, 0x55, 0x04, 0x07, 0x1e, 0x0e, 0x04, 0x1a,
0x04, 0x3e, 0x04, 0x40, 0x04, 0x3e, 0x04, 0x3b,
0x04, 0x35, 0x04, 0x32, 0x31, 0x3b, 0x30, 0x39,
0x06, 0x03, 0x55, 0x04, 0x08, 0x1e, 0x32, 0x00,
0x35, 0x00, 0x30, 0x00, 0x20, 0x00, 0x20, 0x04,
0x1c, 0x04, 0x3e, 0x04, 0x41, 0x04, 0x3a, 0x04,
0x3e, 0x04, 0x32, 0x04, 0x41, 0x04, 0x3a, 0x04,
0x30, 0x04, 0x4f, 0x00, 0x20, 0x04, 0x3e, 0x04,
0x31, 0x04, 0x3b, 0x04, 0x30, 0x04, 0x41, 0x04,
0x42, 0x04, 0x4c, 0x00, 0x20, 0x00, 0x20, 0x00,
0x20, 0x31, 0x0b, 0x30, 0x09, 0x06, 0x03, 0x55,
0x04, 0x06, 0x13, 0x02, 0x52, 0x55, 0x31, 0x27,
0x30, 0x25, 0x06, 0x03, 0x55, 0x04, 0x2a, 0x1e,
0x1e, 0x04, 0x12, 0x04, 0x30, 0x04, 0x3b, 0x04,
0x35, 0x04, 0x40, 0x04, 0x38, 0x04, 0x39, 0x00,
0x20, 0x04, 0x2e, 0x04, 0x40, 0x04, 0x4c, 0x04,
0x35, 0x04, 0x32, 0x04, 0x38, 0x04, 0x47, 0x31,
0x17, 0x30, 0x15, 0x06, 0x03, 0x55, 0x04, 0x04,
0x1e, 0x0e, 0x04, 0x11, 0x04, 0x3b, 0x04, 0x30,
0x04, 0x36, 0x04, 0x3d, 0x04, 0x3e, 0x04, 0x32,
0x31, 0x21, 0x30, 0x1f, 0x06, 0x03, 0x55, 0x04,
0x03, 0x1e, 0x18, 0x04, 0x11, 0x04, 0x3b, 0x04,
0x30, 0x04, 0x36, 0x04, 0x3d, 0x04, 0x3e, 0x04,
0x32, 0x00, 0x20, 0x04, 0x12, 0x00, 0x2e, 0x04,
0x2e, 0x00, 0x2e, 0x31, 0x28, 0x30, 0x26, 0x06,
0x09, 0x2a, 0x86, 0x48, 0x86, 0xf7, 0x0d, 0x01,
0x09, 0x01, 0x16, 0x19, 0x76, 0x62, 0x6c, 0x61,
0x7a, 0x68, 0x6e, 0x6f, 0x76, 0x40, 0x6c, 0x69,
0x73, 0x73, 0x69, 0x2d, 0x63, 0x72, 0x79, 0x70,
0x74, 0x6f, 0x2e, 0x72, 0x75, 0x31, 0x0e, 0x30,
0x0c, 0x06, 0x03, 0x55, 0x04, 0x05, 0x13, 0x05,
0x32, 0x31, 0x37, 0x33, 0x31, 0x30, 0x63, 0x30,
0x1c, 0x06, 0x06, 0x2a, 0x85, 0x03, 0x02, 0x02,
0x13, 0x30, 0x12, 0x06, 0x07, 0x2a, 0x85, 0x03,
0x02, 0x02, 0x24, 0x00, 0x06, 0x07, 0x2a, 0x85,
0x03, 0x02, 0x02, 0x1e, 0x01, 0x03, 0x43, 0x00,
0x04, 0x40, 0xbb, 0xcf, 0x7d, 0xb4, 0x3d, 0xbd,
0x7f, 0x09, 0x11, 0x60, 0xc9, 0xc3, 0x17, 0x16,
0xe4, 0xfe, 0xdd, 0xf3, 0x02, 0x10, 0xdf, 0x77,
0xf1, 0xe1, 0x3c, 0x22, 0x25, 0x6b, 0x1f, 0xeb,
0x07, 0x14, 0xa0, 0x45, 0x99, 0x3d, 0x20, 0x44,
0x44, 0x5d, 0x63, 0xe3, 0x19, 0x8c, 0xc5, 0x65,
0x14, 0xe3, 0x3e, 0x03, 0xe0, 0x2a, 0x91, 0x75,
```

```
0x1b, 0x0e, 0x12, 0x93, 0x7f, 0xdb, 0xcb, 0x72,
0x98, 0xd1, 0xa3, 0x82, 0x03, 0x48, 0x30, 0x82,
0x03, 0x44, 0x30, 0x09, 0x06, 0x03, 0x55, 0x1d,
0x13, 0x04, 0x02, 0x30, 0x00, 0x30, 0x0b, 0x06,
0x03, 0x55, 0x1d, 0x0f, 0x04, 0x04, 0x03, 0x02,
0x05, 0xe0, 0x30, 0x29, 0x06, 0x03, 0x55, 0x1d,
0x25, 0x04, 0x22, 0x30, 0x20, 0x06, 0x08, 0x2b,
0x06, 0x01, 0x05, 0x05, 0x07, 0x03, 0x02, 0x06,
0x08, 0x2b, 0x06, 0x01, 0x05, 0x05, 0x07, 0x03,
0x04, 0x06, 0x0a, 0x2b, 0x06, 0x01, 0x04, 0x01,
0x82, 0x37, 0x14, 0x02, 0x02, 0x30, 0x1d, 0x06,
0x03, 0x55, 0x1d, 0x0e, 0x04, 0x16, 0x04, 0x14,
0xbb, 0xab, 0x03, 0x54, 0xaf, 0x26, 0xae, 0x51,
0x63, 0xa1, 0x5e, 0x12, 0xb6, 0xa3, 0x6d, 0xd5,
0xd8, 0x47, 0xa3, 0xb5, 0x30, 0x82, 0x01, 0x4e,
0x06, 0x03, 0x55, 0x1d, 0x23, 0x04, 0x82, 0x01,
0x45, 0x30, 0x82, 0x01, 0x41, 0x80, 0x14, 0xa2,
0xb8, 0x8c, 0x07, 0x47, 0xa0, 0x1f, 0x88, 0xdd,
0x14, 0x37, 0x6a, 0x13, 0x65, 0x69, 0x3c, 0xde,
0x28, 0xb4, 0xcb, 0xa1, 0x82, 0x01, 0x24, 0xa4,
0x82, 0x01, 0x20, 0x30, 0x82, 0x01, 0x1c, 0x31,
0x1a, 0x30, 0x18, 0x06, 0x08, 0x2a, 0x85, 0x03,
0x03, 0x81, 0x03, 0x01, 0x01, 0x12, 0x0c, 0x30,
0x30, 0x35, 0x30, 0x35, 0x34, 0x30, 0x39, 0x30,
0x38, 0x33, 0x35, 0x31, 0x18, 0x30, 0x16, 0x06,
0x05, 0x2a, 0x85, 0x03, 0x64, 0x01, 0x12, 0x0d,
0x31, 0x30, 0x39, 0x35, 0x30, 0x31, 0x38, 0x30,
0x30, 0x33, 0x34, 0x32, 0x30, 0x31, 0x1e, 0x30,
0x1c, 0x06, 0x03, 0x55, 0x04, 0x07, 0x0c, 0x15,
0xd0, 0xb3, 0x2e, 0xd0, 0xae, 0xd0, 0xb1, 0xd0,
0xb8, 0xd0, 0xbb, 0xd0, 0xb5, 0xd0, 0xb9, 0xd0,
0xbd, 0xd1, 0x8b, 0xd0, 0xb9, 0x31, 0x2f, 0x30,
0x2d, 0x06, 0x03, 0x55, 0x04, 0x08, 0x0c, 0x26,
0x35, 0x30, 0x20, 0xd0, 0x9c, 0xd0, 0xbe, 0xd1,
0x81, 0xd0, 0xba, 0xd0, 0xbe, 0xd0, 0xb2, 0xd1,
0x81, 0xd0, 0xba, 0xd0, 0xb0, 0xd1, 0x8f, 0x20,
0xd0, 0xbe, 0xd0, 0xb1, 0xd0, 0xbb, 0xd0, 0xb0,
0xd1, 0x81, 0xd1, 0x82, 0xd1, 0x8c, 0x31, 0x0b,
0x30, 0x09, 0x06, 0x03, 0x55, 0x04, 0x06, 0x13,
0x02, 0x52, 0x55, 0x31, 0x23, 0x30, 0x21, 0x06,
0x03, 0x55, 0x04, 0x0a, 0x0c, 0x1a, 0xd0, 0x9e,
0xd0, 0x9e, 0xd0, 0x9e, 0x20, 0xd0, 0x9b, 0xd0,
0x98, 0xd0, 0xa1, 0xd0, 0xa1, 0xd0, 0x98, 0x2d,
0xd0, 0xa1, 0xd0, 0xbe, 0xd1, 0x84, 0xd1, 0x82,
```

```
0x31, 0x1e, 0x30, 0x1c, 0x06, 0x03, 0x55, 0x04,
0x0b, 0x0c, 0x15, 0xd0, 0xa2, 0xd0, 0xb5, 0xd1,
0x81, 0xd1, 0x82, 0xd0, 0xbe, 0xd0, 0xb2, 0xd1,
0x8b, 0xd0, 0xb9, 0x20, 0xd0, 0xa3, 0xd0, 0xa6,
0x31, 0x23, 0x30, 0x21, 0x06, 0x03, 0x55, 0x04,
0x03, 0x0c, 0x1a, 0xd0, 0x9e, 0xd0, 0x9e, 0xd0,
0x9e, 0x20, 0xd0, 0x9b, 0xd0, 0x98, 0xd0, 0xa1,
0xd0, 0xa1, 0xd0, 0x98, 0x2d, 0xd0, 0xa1, 0xd0,
0xbe, 0xd1, 0x84, 0xd1, 0x82, 0x31, 0x1c, 0x30,
0x1a, 0x06, 0x09, 0x2a, 0x86, 0x48, 0x86, 0xf7,
0x0d, 0x01, 0x09, 0x01, 0x16, 0x0d, 0x69, 0x6e,
0x66, 0x6f, 0x40, 0x6c, 0x69, 0x73, 0x73, 0x69,
0x2e, 0x72, 0x75, 0x82, 0x01, 0x00, 0x30, 0x24,
0x06, 0x03, 0x55, 0x1d, 0x11, 0x04, 0x1d, 0x30,
0x1b, 0x81, 0x19, 0x76, 0x62, 0x6c, 0x61, 0x7a,
0x68, 0x6e, 0x6f, 0x76, 0x40, 0x6c, 0x69, 0x73,
0x73, 0x69, 0x2d, 0x63, 0x72, 0x79, 0x70, 0x74,
0x6f, 0x2e, 0x72, 0x75, 0x30, 0x18, 0x06, 0x03,
0x55, 0x1d, 0x12, 0x04, 0x11, 0x30, 0x0f, 0x81,
0x0d, 0x69, 0x6e, 0x66, 0x6f, 0x40, 0x6c, 0x69,
0x73, 0x73, 0x69, 0x2e, 0x72, 0x75, 0x30, 0x81,
0xc1, 0x06, 0x05, 0x2a, 0x85, 0x03, 0x64, 0x70,
0x04, 0x81, 0xb7, 0x30, 0x81, 0xb4, 0x0c, 0x24,
0xd0, 0x9f, 0xd0, 0x91, 0xd0, 0x97, 0xd0, 0x98,
0x20, 0xc2, 0xab, 0xd0, 0xa1, 0xd0, 0x9a, 0xd0,
0x97, 0xd0, 0x98, 0x20, 0xc2, 0xab, 0xd0, 0x9b,
0xd0, 0x98, 0xd0, 0xa0, 0xd0, 0xa1, 0xd0, 0xa1,
0xd0, 0x9b, 0xc2, 0xbb, 0x0c, 0x4e, 0xd0, 0x9f,
0xd1, 0x80, 0xd0, 0xbe, 0xd0, 0xb3, 0xd1, 0x80,
0xd0, 0xb0, 0xd0, 0xbc, 0xd0, 0xbc, 0xd0, 0xbd,
0xd0, 0xbe, 0x20, 0xd0, 0xb0, 0xd0, 0xbf, 0xd0,
0xbf, 0xd0, 0xb0, 0xd1, 0x80, 0xd0, 0xb0, 0xd1,
0x82, 0xd0, 0xbd, 0xd1, 0x8b, 0xd0, 0xb9, 0x20,
0xd0, 0xba, 0xd0, 0xbe, 0xd0, 0xbc, 0xd0, 0xbf,
0xd0, 0xbb, 0xd0, 0xb5, 0xd0, 0xba, 0xd1, 0x81,
0x20, 0xc2, 0xab, 0xd0, 0x9b, 0xd0, 0x98, 0xd0,
0xa1, 0xd0, 0xa1, 0xd0, 0x98, 0x2d, 0xd0, 0xa3,
0xd0, 0xa6, 0xc2, 0xbb, 0x0c, 0x1d, 0xd0, 0xa1,
0xd0, 0xa4, 0x2f, 0x31, 0x31, 0x31, 0x2d, 0x31,
0x39, 0x37, 0x39, 0x20, 0xd0, 0xbe, 0xd1, 0x82,
0x20, 0x30, 0x31, 0x2e, 0x30, 0x32, 0x2e, 0x32,
0x30, 0x31, 0x33, 0x0c, 0x1d, 0xd0, 0xa1, 0xd0,
0xa4, 0x2f, 0x31, 0x32, 0x31, 0x2d, 0x31, 0x38,
0x37, 0x30, 0x20, 0xd0, 0xbe, 0xd1, 0x82, 0x20,
```

```
0x32, 0x36, 0x2e, 0x30, 0x36, 0x2e, 0x32, 0x30,
0x31, 0x32, 0x30, 0x2f, 0x06, 0x05, 0x2a, 0x85,
0x03, 0x64, 0x6f, 0x04, 0x26, 0x0c, 0x24, 0xd0,
0x9f, 0xd0, 0x91, 0xd0, 0x97, 0xd0, 0x98, 0x20,
0xc2, 0xab, 0xd0, 0xa1, 0xd0, 0x9a, 0xd0, 0x97,
0xd0, 0x98, 0x20, 0xc2, 0xab, 0xd0, 0x9b, 0xd0,
0x98, 0xd0, 0xa0, 0xd0, 0xa1, 0xd0, 0xa1, 0xd0,
0x9b, 0xc2, 0xbb, 0x30, 0x1d, 0x06, 0x03, 0x55,
0x1d, 0x20, 0x04, 0x16, 0x30, 0x14, 0x30, 0x08,
0x06, 0x06, 0x2a, 0x85, 0x03, 0x64, 0x71, 0x01,
0x30, 0x08, 0x06, 0x06, 0x2a, 0x85, 0x03, 0x64,
0x71, 0x02, 0x30, 0x3a, 0x06, 0x03, 0x55, 0x1d,
0x1f, 0x04, 0x33, 0x30, 0x31, 0x30, 0x2f, 0xa0,
0x2d, 0xa0, 0x2b, 0x86, 0x29, 0x68, 0x74, 0x74,
0x70, 0x3a, 0x2f, 0x2f, 0x63, 0x61, 0x2e, 0x73,
0x6f, 0x66, 0x74, 0x2e, 0x6c, 0x69, 0x73, 0x73,
0x69, 0x2e, 0x72, 0x75, 0x2f, 0x70, 0x75, 0x62,
0x2f, 0x63, 0x72, 0x6c, 0x2f, 0x63, 0x61, 0x63,
0x72, 0x6c, 0x2e, 0x63, 0x72, 0x6c, 0x30, 0x0a,
0x06, 0x06, 0x2a, 0x85, 0x03, 0x02, 0x02, 0x03,
0x05, 0x00, 0x03, 0x41, 0x00, 0x5a, 0xdc, 0xfb,
0xe4, 0x55, 0xed, 0xc8, 0xa6, 0x1e, 0xf2, 0x4b,
0xe8, 0x45, 0xcd, 0x2b, 0x32, 0x30, 0xac, 0xe4,
0x4a, 0x56, 0x23, 0x8c, 0x00, 0xca, 0xc8, 0x83,
0xd1, 0xd0, 0xf3, 0xf0, 0x0c, 0x77, 0x53, 0xd6,
0xc0, 0x2e, 0x72, 0xc7, 0xf4, 0x79, 0x10, 0x4c,
0xba, 0x4b, 0x72, 0xe2, 0x08, 0x34, 0x37, 0x8a,
0xf7, 0x78, 0x64, 0x86, 0xa9, 0x10, 0xfc, 0x95,
0xde, 0x7d, 0x63, 0xe8, 0x16,

CKA_CERTIFICATE_TYPE
0x00, 0x00, 0x00, 0x00,

CKA_ISSUER: length 0

CKA_SERIAL_NUMBER: length 0

CKA_TRUSTED
0x00,

CKA_CERTIFICATE_CATEGORY
0x01, 0x00, 0x00, 0x00,

CKA_SUBJECT
```

```
0x30, 0x82, 0x01, 0x5c, 0x31, 0x1d, 0x30, 0x1b,
0x06, 0x03, 0x55, 0x04, 0x0a, 0x1e, 0x14, 0x04,
0x1b, 0x04, 0x18, 0x04, 0x21, 0x04, 0x21, 0x04,
0x18, 0x00, 0x2d, 0x04, 0x21, 0x04, 0x3e, 0x04,
0x44, 0x04, 0x42, 0x31, 0x39, 0x30, 0x37, 0x06,
0x03, 0x55, 0x04, 0x09, 0x1e, 0x30, 0x04, 0x1b,
0x04, 0x35, 0x04, 0x3d, 0x04, 0x38, 0x04, 0x3d,
0x04, 0x41, 0x04, 0x3a, 0x04, 0x30, 0x04, 0x4f,
0x00, 0x20, 0x00, 0x34, 0x00, 0x2c, 0x00, 0x20,
0x04, 0x3f, 0x04, 0x3e, 0x04, 0x3c, 0x04, 0x35,
0x04, 0x49, 0x04, 0x35, 0x04, 0x3d, 0x04, 0x38,
0x04, 0x35, 0x00, 0x20, 0x00, 0x37, 0x31, 0x17,
0x30, 0x15, 0x06, 0x03, 0x55, 0x04, 0x07, 0x1e,
0x0e, 0x04, 0x1a, 0x04, 0x3e, 0x04, 0x40, 0x04,
0x3e, 0x04, 0x3b, 0x04, 0x35, 0x04, 0x32, 0x31,
0x3b, 0x30, 0x39, 0x06, 0x03, 0x55, 0x04, 0x08,
0x1e, 0x32, 0x00, 0x35, 0x00, 0x30, 0x00, 0x20,
0x00, 0x20, 0x04, 0x1c, 0x04, 0x3e, 0x04, 0x41,
0x04, 0x3a, 0x04, 0x3e, 0x04, 0x32, 0x04, 0x41,
0x04, 0x3a, 0x04, 0x30, 0x04, 0x4f, 0x00, 0x20,
0x04, 0x3e, 0x04, 0x31, 0x04, 0x3b, 0x04, 0x30,
0x04, 0x41, 0x04, 0x42, 0x04, 0x4c, 0x00, 0x20,
0x00, 0x20, 0x00, 0x20, 0x31, 0x0b, 0x30, 0x09,
0x06, 0x03, 0x55, 0x04, 0x06, 0x13, 0x02, 0x52,
0x55, 0x31, 0x27, 0x30, 0x25, 0x06, 0x03, 0x55,
0x04, 0x2a, 0x1e, 0x1e, 0x04, 0x12, 0x04, 0x30,
0x04, 0x3b, 0x04, 0x35, 0x04, 0x40, 0x04, 0x38,
0x04, 0x39, 0x00, 0x20, 0x04, 0x2e, 0x04, 0x40,
0x04, 0x4c, 0x04, 0x35, 0x04, 0x32, 0x04, 0x38,
0x04, 0x47, 0x31, 0x17, 0x30, 0x15, 0x06, 0x03,
0x55, 0x04, 0x04, 0x1e, 0x0e, 0x04, 0x11, 0x04,
0x3b, 0x04, 0x30, 0x04, 0x36, 0x04, 0x3d, 0x04,
0x3e, 0x04, 0x32, 0x31, 0x21, 0x30, 0x1f, 0x06,
0x03, 0x55, 0x04, 0x03, 0x1e, 0x18, 0x04, 0x11,
0x04, 0x3b, 0x04, 0x30, 0x04, 0x36, 0x04, 0x3d,
0x04, 0x3e, 0x04, 0x32, 0x00, 0x20, 0x04, 0x12,
0x00, 0x2e, 0x04, 0x2e, 0x00, 0x2e, 0x31, 0x28,
0x30, 0x26, 0x06, 0x09, 0x2a, 0x86, 0x48, 0x86,
0xf7, 0x0d, 0x01, 0x09, 0x01, 0x16, 0x19, 0x76,
0x62, 0x6c, 0x61, 0x7a, 0x68, 0x6e, 0x6f, 0x76,
0x40, 0x6c, 0x69, 0x73, 0x73, 0x69, 0x2d, 0x63,
0x72, 0x79, 0x70, 0x74, 0x6f, 0x2e, 0x72, 0x75,
0x31, 0x0e, 0x30, 0x0c, 0x06, 0x03, 0x55, 0x04,
0x05, 0x13, 0x05, 0x32, 0x31, 0x37, 0x33, 0x31,
```

```
CKA_ID
0xbb, 0xab, 0x03, 0x54, 0xaf, 0x26, 0xae, 0x51,
0x63, 0xa1, 0x5e, 0x12, 0xb6, 0xa3, 0x6d, 0xd5,
0xd8, 0x47, 0xa3, 0xb5,

CKA_MODIFIABLE
0x01,

CKA_COPYABLE
0x01,

----------------------------------
OK
```

### 2.4.9 Экспорт сертификата

С опцией -outfile сертификат экспортируется в заданный файл. В опции -outform задается формат файла – PEM или DER. По умолчанию, используется формат PEM.

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -outfile pki_out.pem -outform pem
Certificate object 'pki' exported to 'pki_out.pem' file
OK
```

### 2.4.10 Импорт сертификата

С опцией -infile сертификат импортируется на токен из заданного файла. В опции -inform задается формат файла – PEM или DER. По умолчанию, используется формат PEM. Поскольку для любых изменений на токене обычно требуется логин, утилита запрашивает PIN пользователя:

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -infile pki_out.pem -inform pem
Enter token user PIN:
Certificate object 'pki' imported from 'pki_out.pem' file
OK
```

### 2.4.11 Импорт ключевой пары и сертификата

Утилита позволяет импортировать на токен ключевую пару и сертификат из транспортного контейнера PKCS#12, если токен допускает импорт закрытого ключа. С опцией -infile указывается путь к файлу контейнера, а в опции -inform задается формат PFX или P12. Для распаковки контейнера будет запрошен пароль к нему. Поскольку для работы с закрытым ключом требуется логин, утилита затем запрашивает PIN пользователя токена:

```
>p11cert -p11 ls11sw2012 -slot 0 -label pki -infile pki.pfx -inform pfx
Enter pki.pfx container password:
Enter token user PIN:
Keypair and certificate objects 'pki' imported from 'pki.pfx' file
OK
```

# 3 Ссылки

1. Официальный сайт ООО "ЛИССИ-Софт". – http://http://soft.lissi.ru//.

2. Официальный сайт Технического комитета по стандартизации (ТК 26) "Криптографическая защита информации". – https://www.tc26.ru.

3. Расширение PKCS#11 для использования российских криптографических алгоритмов. – Технический комитет по стандартизации (ТК 26) "Криптографическая защита информации". – Москва, ТК 26, 2008.

4. Расширение PKCS#11 для использования российских стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 (готовится к публикации). – Технический комитет по стандартизации (ТК 26) "Криптографическая защита информации". – Москва, ТК 26, 2013.

5. PKCS#11 v2.30: Cryptographic Token Interface Standard. – RSA Laboratories, 2009. – http://www.rsa.com/rsalabs/node.asp?id=2133.