Утверждены решением заседания
технического комитета по стандартизации
«Криптографическая защита информации»
(Протокол № 10 от 27.11.2012 г.)

# Методические рекомендации

## технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)

# Ключевой контейнер

*Дополнение к PKCS#15*

Версия 1.0

## Оглавление

# 1. Общие положения

Данный документ описывает дополнения к стандарту PKCS#15, позволяющие использовать синтаксис данного стандарта для создания контейнеров хранения ключей алгоритмов ГОСТ Р 34-10 2001 и ГОСТ 28147-89.

В соответствии с разделом 4 стандарта PKCS#15 [1] состав и иерархическая структура объектов представляется в виде следующей схемы.

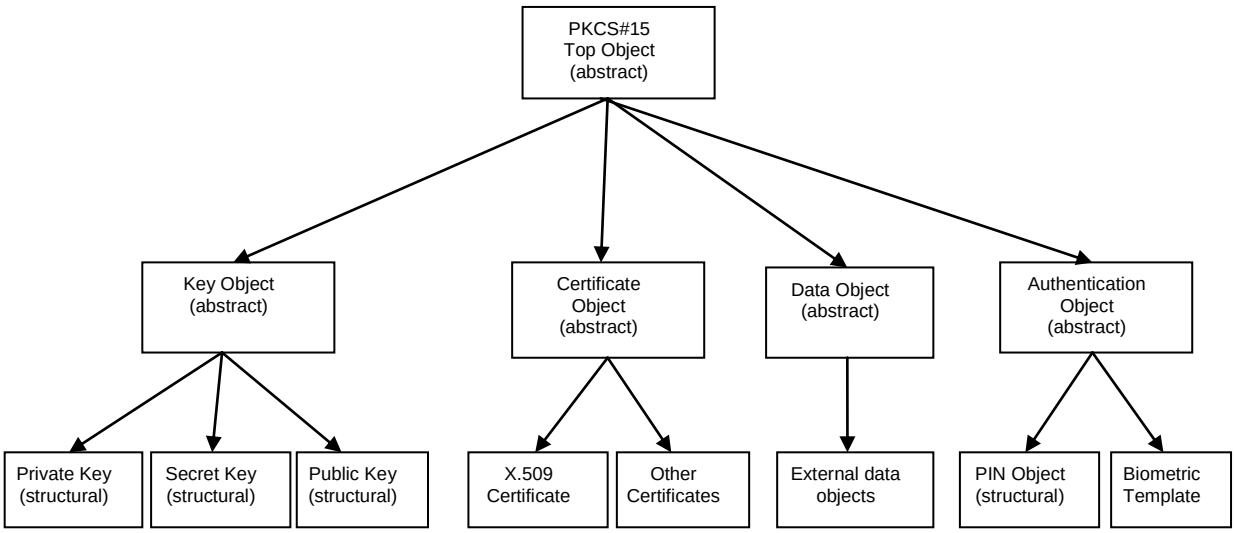


Рис. 1 Состав и иерархическая структура объектов PKCS#15

Как видно из рис.1 существующее в рамках стандарта PKCS#15 множество типов данных покрывает все потребности ключевого контейнера и обеспечивает четкую ссылочную структуру, облегчающую поиск и сопоставление объектов.

Типы данных *Authentication Object* и *Data Object* относятся в большей мере к носителям информации типа *Token* и для программных реализаций не представляют особого интереса. Вместе с тем объект *Data Object* предоставляет возможности для расширений, определяемых производителем. Объекты *Authentication Object* могут быть полезны для хранения политик парольной защиты. Поскольку при совместном использовании контейнера разными СКЗИ данные объекты роли не играют, в данном документе они из рассмотрения исключаются.

Существенной представляется возможность хранения сертификатов различного типа. В настоящий момент в большинстве приложений используются сертификаты формата X.509, но вместе с тем в стандарте предусмотрены возможности хранения и использования сертификатов других типов, в частности атрибутных сертификатов, PGP и других (раздел 6.6 [1]).

# 2. Базовые типы PKCS#15

Базовые типы подробно описаны в разделе 6.1 стандарта PKCS #15 [1]. Фактически, этих типов достаточно для спецификации информации о ключах, включая назначение ключей, сроки действия, данные о владельце, издателе и т.п. Нет смысла

полностью излагать соответствующий раздел стандарта в настоящем документе, но следует рассмотреть отдельные, важные с точки зрения поставленной задачи, типы.

В рамках PKCS#15 [1] не существует понятия имени контейнера, для именования и связывания объектов применяется метка (раздел 6.1.3 PKCS #15 [1]).

**Label ::= UTF8String (SIZE(0..pkcs15-ub-label))**

В идеологии PKCS#15 [1] объекты могут храниться как в виде значений, так и в виде ссылок на другие объекты, например файлы, общие ресурсы и т.д. Для этого применяют тип данных **PathOrObjects** (раздел 6.1.7 PKCS #15 [1]).

Этот же тип позволяет однозначно указать, в каком виде хранятся данные, открытом (**objects [0]**) или зашифрованном (**direct-protected [2]**).

```
PathOrObjects {ObjectType} ::= CHOICE {
path Path,
objects [0] SEQUENCE OF ObjectType,
...,
indirect-protected [1] ReferencedValue {EnvelopedData {SEQUENCE OF
ObjectType}},
direct-protected [2] EnvelopedData {SEQUENCE OF ObjectType},
}
```

Для обеспечения конфиденциальности закрытых ключей логично воспользоваться типом **EnvelopedData: direct-protected [2] EnvelopedData {SEQUENCE OF ObjectType}**.

Для идентификации параметров объектов и области их применения может быть использован тип **KeyInfo** (раздел 6.1.13 PKCS #15 [1]).

```
KeyInfo {ParameterType, OperationsType} ::= CHOICE {
reference Reference,
paramsAndOps SEQUENCE {
parameters ParameterType,
supportedOperations OperationsType OPTIONAL
}
}
```

Сами объекты PKCS#15 [1] представляют собой набор атрибутов разного уровня детализации, позволяющих описывать всевозможные свойства объектов, и при необходимости расширить перечень описываемых свойств.

```
PKCS15Object {ClassAttributes, SubClassAttributes, TypeAttributes} ::=
SEQUENCE {
commonObjectAttributes CommonObjectAttributes,
classAttributes ClassAttributes,
subClassAttributes [0] SubClassAttributes OPTIONAL,
typeAttributes [1] TypeAttributes
}
```

# 3. Объекты для хранения ключей

В рамках стандарта PKCS#15 [1] в контейнере могут храниться ключи трех типов: *Private, Secret* и *Public*. Рассмотрим предлагаемые структуры и возможности их расширения для хранения ключей алгоритмов линейки ГОСТ.

## 3.1. Key Value

Для обеспечения защиты закрытых ключей от утечек по побочным каналам при считывании и проведении операций с ключами, целесообразно использование маскированных ключей. Для хранения маскированных ключей и наборов масок предлагается использовать представление ключа в виде:

**KeyValueMask ::= OCTET STRING { $M_1|M_2|....|M_{k+1}$ }.**

Подробное описание данного представления ключа изложено в документе [7].

## 3.2. Private Key

В соответствии с разделом 6.3.1 PKCS#15 [1].

```
PrivateKeyType ::= CHOICE {
privateRSAKeyPrivateKeyObject {PrivateRSAKeyAttributes},
privateECKey [0] PrivateKeyObject {PrivateECKeyAttributes},
privateDHKey [1] PrivateKeyObject {PrivateDHKeyAttributes},
privateDSAKey[2] PrivateKeyObject {PrivateDSAKeyAttributes},
privateKEAKey[3] PrivateKeyObject {PrivateKEAKeyAttributes},
... -- For future extensions
}
PrivateKeyObject {KeyAttributes} ::= PKCS15Object {
CommonKeyAttributes, CommonPrivateKeyAttributes, KeyAttributes}
```

Для хранения ключей алгоритма ГОСТ 34.10-2001 предлагается ввести соответствующий тип ключа:

```
privateGostR3410-2001Key [26] PrivateKeyObject {PrivateGostR3410-
2001KeyAttributes}
.

PrivateGostR3410-2001KeyAttributes ::= SEQUENCE {
value ObjectValue { GostR3410-2001PrivateKey},
keyInfo KeyInfo {GostPrivateKeyParameters, PublicKeyOperations}
OPTIONAL,
... -- For future extensions
}

GostR3410-2001PrivateKey ::= KeyValueMask

GostPrivateKeyParameters ::= CHOICE {
CryptoProParamSet OBJECT IDENTIFIER,
PrivateKeyParamSet [0] GostR3410-2001-ParamSetParameters,
SecretKeyParamSet [1] Gost28147-89-ParamSetParameters,
```

```
...
}
```

**CryptoProParamSet** - идентификатор параметров алгоритма, который выбирается в соответствии с разделом 8.4 RFC4357 [3].

```
GostR3410-2001-ParamSetAlgorithm ALGORITHM-IDENTIFIER ::= {
  { GostR3410-2001-ParamSetParameters IDENTIFIED BY
      id-GostR3410-2001-TestParamSet } |
  { GostR3410-2001-ParamSetParameters IDENTIFIED BY
      id-GostR3410-2001-CryptoPro-A-ParamSet  } |
  { GostR3410-2001-ParamSetParameters IDENTIFIED BY
      id-GostR3410-2001-CryptoPro-B-ParamSet  } |
  { GostR3410-2001-ParamSetParameters IDENTIFIED BY
      id-GostR3410-2001-CryptoPro-C-ParamSet  } |
  { GostR3410-2001-ParamSetParameters IDENTIFIED BY
      id-GostR3410-2001-CryptoPro-XchA-ParamSet  } |
  { GostR3410-2001-ParamSetParameters IDENTIFIED BY
      id-GostR3410-2001-CryptoPro-XchB-ParamSet  }
}
```

Структура **GostR3410-2001-ParamSetParameters** определена в разделе 8.4 RFC4357 [3], структура **Gost28147-89-ParamSetParameters** – в разделе 8.1 RFC4357 [3].

Если **keyInfo** не указано, предполагается значение параметров по умолчанию:

**KeyInfo.paramsAndOps.parameters = id-GostR3410-2001-CryptoPro-A-ParamSet**

## 3.3. Public Key

Аналогично закрытому ключу в разделе 6.4.1 PKCS #15 [1] определены открытые ключи.

```
PublicKeyType ::= CHOICE {
publicRSAKey PublicKeyObject {PublicRSAKeyAttributes},
publicECKey [0] PublicKeyObject {PublicECKeyAttributes},
publicDHKey [1] PublicKeyObject {PublicDHKeyAttributes},
publicDSAKey [2] PublicKeyObject {PublicDSAKeyAttributes},
publicKEAKey [3] PublicKeyObject {PublicKEAKeyAttributes},
… -- For future extensions
}
PublicKeyObject {KeyAttributes} ::= PKCS15Object {
      CommonKeyAttributes, CommonPublicKeyAttributes, KeyAttributes}
```

Для хранения открытого ключа, аналогично секретному, предлагается использовать следующий тип.

```
publicGostR3410-2001Key [26] PublicKeyObject {PublicGostR3410-
2001KeyAttributes},
```

**PublicGostR3410-2001KeyAttributes ::= SEQUENCE {**
**value ObjectValue {ECPublicKeyChoice},**
**keyInfo KeyInfo {GostPrivateKeyParameters, PublicKeyOperations} OPTIONAL,**
**... -- For future extensions**
**}**

**GostR3410-2001PublicKeyChoice ::= CHOICE {**
**raw GostR3410-2001Point,**
**spki SubjectPublicKeyInfo, -- See X.509. Must contain a public EC key**
**...**
**}**

При использовании **SubjectPublicKeyInfo** открытый ключ и его параметры должны быть представлены в соответствии с разделом 2.3.2 RFC4491 [4].

При использовании **GostR3410-2001Point** открытый ключ должен иметь представление, описанное в документе [7].

**GostR3410-2001Point ::= GostR3410-2001-PublicKey.**

Если **keyInfo** не указано, предполагается значение параметров по умолчанию:

**KeyInfo.paramsAndOps.parameters = id-GostR3410-2001-CryptoPro-A-ParamSet.**

## 3.4. Secret Key

Структура симметричного секретного ключа определена в разделе 6.5.1 PKCS #15 [1].

**SecretKeyType ::= CHOICE {**
**genericSecretKey SecretKeyObject {GenericSecretKeyAttributes},**
**rc2key [0] SecretKeyObject {GenericSecretKeyAttributes},**
**rc4key [1] SecretKeyObject {GenericSecretKeyAttributes},**
**desKey [2] SecretKeyObject {GenericSecretKeyAttributes},**
**des2Key [3] SecretKeyObject {GenericSecretKeyAttributes},**
**des3Key [4] SecretKeyObject {GenericSecretKeyAttributes},**
**castKey [5] SecretKeyObject {GenericSecretKeyAttributes},**
**cast3Key [6] SecretKeyObject {GenericSecretKeyAttributes},**
**cast128Key [7] SecretKeyObject {GenericSecretKeyAttributes},**
**rc5Key [8] SecretKeyObject {GenericSecretKeyAttributes},**
**ideaKey [9] SecretKeyObject {GenericSecretKeyAttributes},**
**skipjackKey [10] SecretKeyObject {GenericSecretKeyAttributes},**
**batonKey [11] SecretKeyObject {GenericSecretKeyAttributes},**
**juniperKey [12] SecretKeyObject {GenericSecretKeyAttributes},**
**rc6Key [13] SecretKeyObject {GenericSecretKeyAttributes},**
**otherKey [14] OtherKey,**
**... -- For future extensions**
**}**
**SecretKeyObject {KeyAttributes} ::= PKCS15Object {**
**CommonKeyAttributes, CommonSecretKeyAttributes, KeyAttributes}**

В данном случае для алгоритма ГОСТ 28147-89 может быть использован тип.

**gostKey [26] GostSecretKey**

```
GostSecretKey ::= SEQUENCE {
keyTypeGost OBJECT IDENTIFIER,
keyAttr SecretKeyObject {GostSecretKeyAttributes}
}
```

В качестве идентификатора типа ключа должен быть представлен идентификатор алгоритма в соответствии с RFC4357 [3].

**keyTypeGost = id-Gost28147-89.**

Атрибуты симметричного ключа определены следующим образом.

```
GostSecretKeyAttributes ::= SEQUENCE {
value KeyValueMask,
keyInfo KeyInfo {GostSecretKeyParameters, SecretKeyOperations}
OPTIONAL,
}

GostSecretKeyParameters ::= CHOICE {
CryptoProParamSet OBJECT IDENTIFIER,
PrivateKeyParamSet [0] GostR3410-2001-ParamSetParameters,
SecretKeyParamSet [1]Gost28147-89-ParamSetParameters,
...
}
```

Идентификаторы параметров алгоритма **CryptoProParamSet** выбираются в соответствии с разделом 8.1 RFC4357 [3].

Если **keyInfo** не указано, принимается по умолчанию.

**KeyInfo.paramsAndOps.parameters = id-Gost28147-89-CryptoPro-A-ParamSet.**

## 4. Обеспечение конфиденциальности ключей

Для обеспечения конфиденциальности объектов *Private* и *Secret Key* в соответствии с PKCS#15 используется тип **EnvelopedData** в соответствии с разделом 6 RFC5652 [2].

```
EnvelopedData {Type} ::= SEQUENCE {
version INTEGER {v0(0), v1(1), v2(2), v3(3), v4(4)}(v0|v1|v2,…),
originatorInfo [0] OriginatorInfo OPTIONAL,
recipientInfos RecipientInfos,
encryptedContentInfo EncryptedContentInfo{Type},
unprotectedAttrs [1] SET SIZE (1..MAX) OF Attribute OPTIONAL
}
```

Зашифрованное содержимое контейнера представляется в виде:

```
EncryptedContentInfo {Type} ::= SEQUENCE {
contentType OBJECT IDENTIFIER,
```

**contentEncryptionAlgorithm AlgorithmIdentifier {{ContentEncryptionAlgorithms}},**
**encryptedContent [0] OCTET STRING OPTIONAL**
**}(CONSTRAINED BY {-- 'encryptedContent' shall be the result of encrypting DER-encoded**
**-- value of type – Type})**

Тип данных, в соответствии с PKCS#15 идентифицируется как:

**pkcs15-ct-PKCS15Token OBJECT IDENTIFIER ::= {pkcs15-ct 1}, где**

**pkcs15 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)**

**pkcs-15(15)},**

**pkcs15-ct OBJECT IDENTIFIER ::= {pkcs15 3} -- Content type branch**

При шифровании должен использоваться алгоритм ГОСТ 28147-89. Алгоритм и параметры шифрования **contentEncryptionAlgorithm** указываются в соответствии с разделом 5.1 RFC4490 [5].

Кроме того, могут использоваться алгоритмы с завершающей имитовставкой:

Алгоритм гаммирования с обратной связью:

```
id-Gost28147-89-cbc-imm OBJECT IDENTIFIER ::=
      { iso(1) member-body(2) ru(643) rans(2) infotecs(4)
        algorithms(3) gost28147-89(2) cbc-imm(2) }
```

Алгоритм гаммирования:

```
id-Gost28147-89-cnt-imm OBJECT IDENTIFIER ::=
      { iso(1) member-body(2) ru(643) rans(2) infotecs(4)
        algorithms(3) gost28147-89(2) cnt-imm(3) }
```

Параметры алгоритмов с завершающей имитовставкой указываются в соответствии с разделом 5.1. RFC4490 [5]. Зашифрованные данные содержат результат зашифрования конкатенированные с имитовставкой, вычисленной на тех же параметрах, что и при зашифровании.

В качестве ключа шифрования (Key Encryption Key, KEK) используется симметричный ключ ГОСТ 28147-89. Информация о ключе шифрования размещается в структуре **RecipientInfo:** .

**RecipientInfo ::= CHOICE {**
**ktri KeyTransRecipientInfo,**
**kari [1] KeyAgreeRecipientInfo,**
**kekri [2] KEKRecipientInfo,**
**pwri [3] PasswordRecipientinfo,**
**ori [4] OtherRecipientInfo }**

Информация о шифровании в этом случае может быть представлена как в виде **kekri,** так и в виде **pwri** (разделы 6.2.3 и 6.2.4 RFC5652 [2] соответственно) .

```
KEKRecipientInfo ::= SEQUENCE {
version CMSVersion, -- always set to 4
kekid KEKIdentifier,
keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
encryptedKey EncryptedKey }

PasswordRecipientInfo ::= SEQUENCE {
version CMSVersion, -- Always set to 0
keyDerivationAlgorithm [0] KeyDerivationAlgorithmIdentifier OPTIONAL,
keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
encryptedKey EncryptedKey }
```

При использовании варианта **pwri** поле **keyDerivationAlgorithm** описывает алгоритм и параметры выработки ключа из пароля пользователя в соответствии с рекомендациями PKCS#5 по схеме PBKDF2 с использованием ГОСТ Р 34.11-94 в соответствии с дополнениями [6].

При шифровании ключа должен использоваться алгоритм ГОСТ 28147-89. Алгоритм и параметры шифрования **keyEncryptionAlgorithm** указываются в соответствии с разделом 5.1 RFC4490 [5].

Зашифрованный ключ представляется в виде:

```
Gost28147-89-EncryptedKey ::=   SEQUENCE {
encryptedKey        Gost28147-89-Key,
maskKey             [0] IMPLICIT Gost28147-89-Key OPTIONAL,
macKey              Gost28147-89-MAC }
```

## 5. Обеспечение целостности информации

Для обеспечения целостности ключей результирующая структура **PKCS15Token** инкапсулируется в **Authenticated-data** в соответствии с разделом 9 RFC5652 [2] с использованием алгоритма HMAC_GOSTR3411.

```
AuthenticatedData ::= SEQUENCE {
version CMSVersion,
originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
recipientInfos RecipientInfos,
macAlgorithm MessageAuthenticationCodeAlgorithm,
digestAlgorithm [1] DigestAlgorithmIdentifier OPTIONAL,
encapContentInfo EncapsulatedContentInfo,
authAttrs [2] IMPLICIT AuthAttributes OPTIONAL,
mac MessageAuthenticationCode,
unauthAttrs [3] IMPLICIT UnauthAttributes OPTIONAL }
```

При этом идентификатор и параметры алгоритма

```
MessageAuthenticationCodeAlgorithm  ::= AlgorithmIdentifier
```

Задаются в соответствии с RFC4490 [5].

**MessageAuthenticationCodeAlgorithm.algorithm = id-HMACGostR3411-94**

Алгоритм ГОСТ Р 34.11-94 при вычислении HMAC используется только с параметрами id-GostR3411-94-CryptoProParamSet, параметры HMAC_GOSTR3411 не указываются:

**MessageAuthenticationCodeAlgorithm. parameters = NULL.**

## 6. Общая структура токена

В соответствии с разделом 7.3 PKCS #15 [1] SoftwareToken представляется в виде следующей структуры:

```
PKCS15Token ::= SEQUENCE {
version INTEGER {v1(0)} (v1,...),
keyManagementInfo [0] KeyManagementInfo OPTIONAL,
pkcs15Objects SEQUENCE OF PKCS15Objects
}

KeyManagementInfo ::= SEQUENCE OF SEQUENCE {
keyId Identifier,
keyInfo CHOICE {
recipientInfo RecipientIInfo,
passwordInfo [0] PasswordInfo
}
} (CONSTRAINED BY {-- Each keyID must be unique --})
PasswordInfo ::= SEQUENCE {
hint Label OPTIONAL,
algId AlgorithmIdentifier {{KeyDerivationAlgorithms}},
...
} (CONSTRAINED BY {--keyID shall point to a KEKRecipientInfo--})
```

Заметим, что при использовании представления информации в виде **pwri** в **KeyManagementInfo** фактически дублируется информация о шифровании ключа в структуре **EnvelopedData.** Данная информация может опционально использоваться для выбора и предварительной проверки пароля в случае, если для разных объектов используются разные пароли.

При использовании представления **kekri** идентификаторы в таблице ключей **keyId** обеспечивают однозначное сопоставление параметров выработки парольного ключа и ключа, зашифрованного на данном пароле в структуре **KEKRecipientInfo.**

Для обеспечения целостности структура **PKCS15Token** может быть инкапсулирована в **AuthenticatedData** или **SignedData,** см. [2]. При этом поле **AuthenticatedData. recipientInfos** может ссылаться на один из **keyId** в таблице ключей инкапсулированной структуры **PKCS15Token. keyManagementInfo.**

## 7. Пример

В данном примере приводится значение Software Token, содержащего:

- начальное заполнение ДСЧ;
- корневой сертификат;
- список отзыва;
- сертификат пользователя 1;
- закрытый ключ пользователя 1
- закрытый ключ пользователя 2;
- открытый ключпользователя 2;
- секретные произвольные данные;
- открытые произвольные данные.

Для защиты секретных данных и обеспечения целостности контейнера используется пароль «123» (шестнадцатиричное представление - 31 32 33).

Значение SoftwareToken в Base64 представлении:


```
MIIVHAIBADFZolcCAQQwBgQEAAAABDAeBgcqhQMCAg0BMBMGByqFAwICHwEECHS67qC+y3deBCow
KAQgXrHRtkIaAt4LxvyMPo2BDd+NRAhdVO9+onduGdo+eKEEBDmTqA0wCAYGKoUDAgIKoQgGBiqF
AwICCTCCFDYGCiqGSIb3DQEPAwGgghQmBIIUIjCCFB4CAQCgTDBKBAQAAAAEoEIwQAYJKoZIhvcN
AQUMMDMEIPRTgEWwL8jG3qoB7aUWId2xZfsfU6vJTB1ks70/2dgMAgIH0AIBIDAIBgYqhQMCAgow
ghPJp4IBbaCCAWmhQDAWDBFGYWN0b3ItVFMgdmVyc2lvbgMBADANBgsrBgEEAegAg3cBA6EXBgsr
BgEEAegAg3cBA6AIMAYCAQKAAQChggEjMBcMEVJhbmRvbSBJbml0IFZhbHVlAwIGwDANBgsrBgEE
AegAg3cBAaGB+AYLKwYBBAHoAIN3AQGigegCAQIxWaJXAgEEMAYEBAAAAAQwHgYHKoUDAgINATAT
BgcqhQMCAh8BBAh0cHBSEiqAUAQqMCgEIF1/hQ8YCiCl+ie81BN3Oa+jUdvnPLOIgLu+uEFbQkYo
BARaaXnNMIGHBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIwEwQI3Y7IAA/KEYgGByqFAwICHwGAWZOb
mDhwSnPdoK6vh0xKAK1iuCGqXInC/5IcXENAVLy2qijTFIvpb2LyBjdpJSxdCckmRBQjUYXdmQaV
Ao4LmL71RlXPY9jlSH1jJXUr9LGT5j4iqtvcRgORpYID/aCCA/kwggP1MBsMFlJvb3QgQ2VydGlm
aWNhdGUgb2YgQ0EDAQAwCQQEAAAAAQEB/6GCA8mgggK5MIICaKADAgECAhAHSLrFkOrFm0xPD+cE
mJyoMAgGBiqFAwICAzB6MSMwIQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkG
A1UEBhMCUlUxDzANBgNVBAcTBk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQ
cm9tbzERMA8GA1UEAxMITWF4aW0gVUMwHhcNMTIwMzIxMTIzOTM4WhcNMTcwMzIxMTI0NjEyWjB6
MSMwIQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUxDzANBgNV
BAcTBk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQcm9tbzERMA8GA1UEAxMI
TWF4aW0gVUMwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUDAgIeAQNDAARAl8vdQt+AKBOymRFk
a+E4EgIfboNfszWxSBXgQ812JG2NcFIQuGFHQM/iMU5UUTnVzyO7JEdZJy/XnfRCqMTdnKOBxzCB
xDALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUw5msLvj2/PBiLIqANd/a
YygX7+0wcwYDVR0fBGwwajBooGagZIYwaHR0cDovL3ZvZW5tZWgtZDBmMjg2YS9DZXJ0RW5yb2xs
L01heGltJTIwVUMuY3JshjBmaWxlOi8vXFx2b2VubWVoLWQwZjI4NmFcQ2VydEVucm9sbFxNYXhp
bSBVQy5jcmwwEAYJKwYBBAGCNxUBBAMCAQAwCAYGKoUDAgIDA0EAwXTg/ChvhJy6+iTto6vRRJfU
4kZ0wtSeufgbUxyYuqqV2+vadqJFLwWZ8Zazny/xceUSZsvrWTky9Xtq0Hz4rTB6MSMwIQYJKoZI
hvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUxDzANBgNVBAcTBk1vc2Nv
dzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQcm9tbzERMA8GA1UEAxMITWF4aW0gVUOg
fDB6MSMwIQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUxDzAN
BgNVBAcTBk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQcm9tbzERMA8GA1UE
AxMITWF4aW0gVUMCEAdIusWQ6sWbTE8P5wSYnKinggN4oIIDdKGCA3AwEAwLQ1JMIGZyb20gQ0ED
AQAwDQYLKwYBBAHoAIN3AQKhggNLBgsrBgEEAegAg3cBAqCCAzowggM2BAQAAAABoHwwejEjMCEG
CSqGSIb3DQEJARYUbWl2YW5vdkBmYWN0b3ItdHMucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZN
b3Njb3cxEjAQBgNVBAoTCUNyeXB0b1BybzEOMAwGA1UECxMFUHJvbW8xETAPBgNVBAMTCE1heGlt
IFVDMIICrjCCAl0CAQEwCAYGKoUDAgIDMHoxIzAhBgkqhkiG9w0BCQEWFG1pdmFub3ZAZmFjdG9y
LXRzLnJ1MQswCQYDVQQGEwJSVTEPMA0GA1UEBxMGTW9zY293MRIwEAYDVQQKEwlDcnlwdG9Qcm8x
DjAMBgNVBAsTBVByb21vMREwDwYDVQQDEwhNYXhpbSBVQxcNMTIwNTE1MDkxMDA2WhcNMTIwNTIy
MjEzMDA2WjCBgTApAgphBNZnAAAAAAASFw0xMjA1MDIxMTQxMjdaMAwwCgYDVR0VBAMKAQUwKQIK
YRBfpgAAAAAABxcNMTIwNTAyMTEzODIwWjAMMAoGA1UdFQQDCgEFMCkCCmHpQqkAAAAAABEXDTEy
MDUwMjExMzgwNVowDDAKBgNVHRUEAwoBBaCCAS4wggEqMB8GA1UdIwQYMBaAFMOZrC749vzwYiyK
gDXf2mMoF+/tMBAGCSsGAQQBgjcVAQQDAgEAMAoGA1UdFAQDAgEFMBwGCSsGAQQBgjcVBAQPFw0x
MjA1MjIwOTIwMDZaMIHKBgkrBgEEAYI3FQ4EgbwwgbkwgbaggbOggbCGga1sZGFwOi8vL0NOPU1h
eGltJTIwVUMsQ049dm9lbmllaC1kMGYyODZhLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2
aWNlcyxDTj1TZXJ2aWNlcyxEQz1VbmF2YWlsYWJsZUNvbmZpZ0ROP2NlcnRpZmljYXRlUmV2b2Nh
dGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDAIBgYqhQMCAgMD
QQBwtkKKmuMFgp5/W5eharGE+/gj5/LNAqMCkuhTg49R9IikDDfGnTxLqww6oQwLfwI1AneI0qME
/Wfsm5Kwg6tXoIICJ6CCAiO6ggIfMCMMHVByaXZhdGUgS2V5IG9mIEFuZHJleSBGZWRvdG92AwIH
gDAxBAQAAAACAwMGZEADAgXgGA8yMDEyMDUxODExMDMwMFqADzIwMTMwNTE4MTExMjAwWqCBvTCB
ujEjMCEGCSqGSIb3DQEJARYUZmVkb3RvdkBmYWN0b3ItdHMucnUxCzAJBgNVBAYTAlJVMRUwEwYD
VQQHHgwEHAQ+BEEEOgQyBDAxGzAZBgNVBAoeEgQkBDAEOgRCBD4EQAAtBCIEITERMA8GA1UECx4I
BCIENQRBBEIxPzA9BgNVBAMeNgQkBDUENAQ+BEIEPgQyACAEEAQ9BDQEQAQ1BDkAIAQSBDsEMAQ0
BDgEPAQ4BEAEPgQyBDgER6GCAQOigfUCAQIxWaJXAgEEMAYEBAAAAAQwHgYHKoUDAgINATATBgcq
hQMCAh8BBAg/O/ihDX+2gwQqMCgEIBCohMMsFi8vPkaX1UVwDW2DrqPLVlXQw3UWwlQs2iFWBAQ3
CD5tMIGUBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIwEwQIozJgvOQgdDAGByqFAwICHwGAZvfwQfzF
FMttKu+iXtLTFxXblpti9lAggi0aHq7OP+RvQZZmaESftaKYj7yuYYa5/d/5gTNHCDIgD3tOGKAM
3XKp0ugeu4pBC4jrqIdrTj0NRrI3SmUAbYIK1VLz2rtLGQle22D4zjAJBgcqhQMCAiMBpIIFQqCC
BT4wggU6MCIMHUNlcnRpZmljYXRlIG9mIEFuZHJleSBGZWRvdG92AwEAMAYEBAAAAAKhggUKoIID
vzCCA26gAwIBAgIKYUp2IgAAAAAAHTAIBgYqhQMCAgMwejEjMCEGCSqGSIb3DQEJARYUbWl2YW5v
dkBmYWN0b3ItdHMucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxEjAQBgNVBAoTCUNy
```

```
eXB0b1BybzEOMAwGA1UECxMFUHJvbW8xETAPBgNVBAMTCE1heGltIFVDMB4XDTEyMDUxODExMDMw
MFoXDTEzMDUxODExMTIwMFowgboxIzAhBgkqhkiG9w0BCQEWFGZlZG90b3ZAZmFjdG9yLXRzLnJ1
MQswCQYDVQQGEwJSVTEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMRswGQYDVQQKHhIEJAQwBDoEQgQ+
BEAALQQiBCExETAPBgNVBAseCAQiBDUEQQRCMT8wPQYDVQQDHjYEJAQ1BDQEPgRCBD4EMgAgBBAE
PQQ0BEAENQQ5ACAEEgQ7BDAENAQ4BDwEOARABD4EMgQ4BEcwYzAcBgYqhQMCAhMwEgYHKoUDAgIj
AQYHKoUDAgIeAQNDAARA7ZIDZgAQEbmsMmgoVnaV0kuxHyJmgvxTzJHKagoUMGcnalND0eKTFksh
ABKJR8iG+SFElVEIp0XmF4VzdZ1kTqOCAZEwggGNMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAK
BggrBgEFBQgCAjAdBgNVHQ4EFgQUUlitDEVDDeX23jl7dzs9+R1p/zkwHwYDVR0jBBgwFoAUw5ms
Lvj2/PBiLIqANd/aYygX7+0wdQYDVR0fBG4wbDBqoGigZoYwaHR0cDovL3ZvZW5tZWgtZDBmMjg2
YS9DZXJ0RW5yb2xsL01heGltJTIwVUMuY3JshjJmaWxlOi8vXFx2b2VubWVoLWQwZjI4NmFcQ2Vy
dEVucm9sbFxNYXhpbSUyMFVDLmNybDCBrgYIKwYBBQUHAQEEgaEwgZ4wTAYIKwYBBQUHMAKGQGh0
dHA6Ly92b2VubWVoLWQwZjI4NmEvQ2VydEVucm9sbC92b2VubWVoLWQwZjI4NmFfTWF4aW0lMjBV
Qy5jcnQwTgYIKwYBBQUHMAKGQmZpbGU6Ly9cXHZvZW5tZWgtZDBmMjg2YVxDZXJ0RW5yb2xsXHZv
ZW5tZWgtZDBmMjg2YV9NYXhpbSUyMFVDLmNydDAIBgYqhQMCAgMDQQBx2yNnJZzJ0IYqyR3znarI
UbypLLr0gvP0js8MgXenLzU0itibsbAKGFCifs+KbcteUyGICOzzyno2Ao2i8fXkMIG6MSMwIQYJ
KoZIhvcNAQkBFhRmZWRvdG92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUxFTATBgNVBAceDAQc
BD4EQQQ6BDIEMDEbMBkGA1UECh4SBCQEMAQ6BEIEPgRAAC0EIgQhMREwDwYDVQQLHggEIgQ1BEEE
QjE/MD0GA1UEAx42BCQENQQ0BD4EQgQ+BDIAIAQQBD0ENARABDUEOQAgBBIEOwQwBDQEOAQ8BDgE
QAQ+BDIEOARHoHwwejEjMCEGCSqGSIb3DQEJARYUbWl2YW5vdkBmYWN0b3ItdHMucnUxCzAJBgNV
BAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxEjAQBgNVBAoTCUNyeXB0b1BybzEOMAwGA1UECxMFUHJv
bW8xETAPBgNVBAMTCE1heGltIFVDAgphSnYiAAAAAAAdoIIBQKCCATy6ggE4MB8MGU5ldyBHZW5l
cmF0ZWQgUHJpdmF0ZSBLZXkDAgeAMA4EBAAAAAMDAgUgAwIF4KGCAQOigfUCAQIxWaJXAgEEMAYE
BAAAAAQwHgYHKoUDAgINATATBgcqhQMCAh8BBAgmMEdynON0bwQqMCgEINa5lZXdetbD5n38Uhlu
xjVOPpUL3iPBI8t2YZjkLnUZBAT9tb2SMIGUBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIwEwQIZFnn
xxTeCuMGByqFAwICHwGAZhf6UWp+DFnz6HLwe42+PfHWds/RGMkAfbGQd+RvaBAn1F0RpI51wSDb
nHOkipM86iaezz4GQeYCxAu2yc0FBk61KxJ0Cb5FTeKYjM9m/F9XBz2yQYu5toX+D9R/e9Lg7zIs
YoP0BzAJBgcqhQMCAiMCoYGSoIGPuoGMMC0MKFB1YmxpYyBLZXkgZm9yIE5ldyBHZW5lcmF0ZWQg
UHJpdmF0ZSBLZXkDAQAwCgQEAAAAAwMCAQKhT6BCBEAei879fJXoTxHjWhSgWP1byz4kiTrekVmZ
6ydbo6+vHdTVjWwyomTTiubNB1QMdntBXmRUC+kjAqf06vplzfZLMAkGByqFAwICIwKnggEgoIIB
HKGCARgwFQwPVG9wLXNlY3JldCBEYXRhAwIGwDANBgsrBgEEAegAg3cBBKGB7wYFKYNIvVKigeUC
AQIxWaJXAgEEMAYEBAAAAAQwHgYHKoUDAgINATATBgcqhQMCAh8BBAhyH/U1lSLswgQqMCgEIPLS
7uYSRGQglx8Cp9IMxdV3RpbwPfi1Yj2pRQrm321kBATiCn8CMIGEBgkqhkiG9w0BBwEwHwYIKoUD
AgQDAgIwEwQIP5CWe/g/MB0GByqFAwICHwGAVhWdwY9iB3DQAzF036cCXNkiPPKXqtXU8cXnBgRk
+XMuZLRbwlBKUmSwqfsHJ/U3WO9NsL2jaaGodywVJY5QB4/gyhTv9jrBFhl2yTHbozdtlvaMgWto
p2ugaaFnMBEMC1B1YmxpYyBEYXRhAwIGQDANBgsrBgEEAegAg3cBBKFDBgYphX2DMAGgOQQ3VGhp
cyBpcyBzb21lIG9wZW4gZGF0YS4gVGhlcmUncyBubyBuZWVkIHRvIGVuY3J5cHQgaXQuAKJMMBkG
CSqGSIb3DQEJAzEMBgoqhkiG9w0BDwMBMC8GCSqGSIb3DQEJBDEiBCBkTtHa7dftuwrYHE6oA05B
+QSn0AIVIzqDnH7usL50aAQg+v1NDmN/KRFZHV0/r6YMxOfxNi6TWeJc1WjlsPpbFTk=
```

Нотация ASN, используемая при формировании данного примера:

```
PKCS15
-- {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-15(15) modules(1) pkcs-15(1)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


P15-AuthenticatedData ::= SEQUENCE {
        version               P15-CMSVersion, -- = 0
        originatorInfo                [0] IMPLICIT P15-OriginatorInfo OPTIONAL, -- not used
        recipientInfos                P15-RecipientInfos,
        macAlgorithm          P15-MessageAuthenticationCodeAlgorithm,
        digestAlgorithm       [1] P15-DigestAlgorithmIdentifier OPTIONAL, -- must be
        encapContentInfo      P15-EncapsulatedContentInfo,
        authAttrs             [2] IMPLICIT P15-AuthAttributes OPTIONAL, -- must be
        mac                   P15-MessageAuthenticationCode,
        unauthAttrs [3]       IMPLICIT P15-UnauthAttributes OPTIONAL  -- not used
}

P15-CMSVersion ::= INTEGER { v0(0), v1(1), v2(2), v3(3), v4(4), v5(5) }

P15-RecipientInfos ::= SET SIZE (1..MAX) OF P15-RecipientInfo

P15-RecipientInfo ::= CHOICE {
       ktri    P15-KeyTransRecipientInfo,           -- not used
       kari    [1] P15-KeyAgreeRecipientInfo,       -- not used
       kekri   [2] P15-KEKRecipientInfo,            -- used by KeyManagement.PasswordInfo
       pwri    [3] P15-PasswordRecipientInfo,       -- not used
       ori     [4] P15-OtherRecipientInfo           -- not used
}

P15-KEKRecipientInfo ::= SEQUENCE {
        version P15-CMSVersion,  -- = 4
        kekid P15-KEKIdentifier,
```

```
        keyEncryptionAlgorithm P15-KeyEncryptionAlgorithmIdentifier,
        encryptedKey P15-EncryptedKey
}

P15-KEKIdentifier ::= SEQUENCE {
        keyIdentifier OCTET STRING,  -- should refer to PasswordInfo keyid
        date GeneralizedTime OPTIONAL,      -- not used
        other P15-OtherKeyAttribute OPTIONAL -- not used
}

P15-KeyEncryptionAlgorithmIdentifier ::= P15-GostKeyWrapAlgorithmIdentifier

P15-GostKeyWrapAlgorithmIdentifier ::= SEQUENCE {
       algorithm      OBJECT IDENTIFIER,
-- must be { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) keyWrap(13) cryptoPro(1) }
       parameters     ANY OPTIONAL
-- must be present and should be Gost28147-89-KeyWrapParameters
}

P15-Gost28147-89-KeyWrapParameters ::= SEQUENCE {
       encryptionParamSet P15-Gost28147-89-ParamSet,
       ukm     OCTET STRING (SIZE (8)) OPTIONAL -- must be present
}

P15-Gost28147-89-ParamSet ::= OBJECT IDENTIFIER
-- may be:
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) encrypts(31) cryptopro-A(1) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) encrypts(31) cryptopro-B(2) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) encrypts(31) cryptopro-C(3) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) encrypts(31) cryptopro-D(4) }


P15-EncryptedKey ::= OCTET STRING -- encapsulates DER of Gost28147-89-EncryptedKey

P15-Gost28147-89-EncryptedKey ::= SEQUENCE {
       encryptedKey P15-Gost28147-89-Key,
       maskKey [0] IMPLICIT P15-Gost28147-89-Key OPTIONAL, -- must be absent
       macKey P15-Gost28147-89-MAC
}

P15-Gost28147-89-Key ::= OCTET STRING (SIZE (32))

P15-Gost28147-89-MAC ::= OCTET STRING (SIZE (1..4))

P15-MessageAuthenticationCodeAlgorithm ::= P15-HmacGostR3411Algorithm

P15-HmacGostR3411Algorithm ::= SEQUENCE {
       algorithm      OBJECT IDENTIFIER,
-- should be { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) hmacgostr3411(10) }
       parameters     ANY OPTIONAL -- must be NULL or absent
}

P15-DigestAlgorithmIdentifier ::= P15-GostR3411Algorithm

P15-GostR3411Algorithm ::= SEQUENCE {
       algorithm      OBJECT IDENTIFIER,
-- should be { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) gostr3411(9) }
       parameters     ANY OPTIONAL -- must be NULL or absent
}

P15-EncapsulatedContentInfo ::= SEQUENCE {
       eContentType   OBJECT IDENTIFIER, -- should be 1.2.840.113549.1.15.3.1
       eContent       [0] EXPLICIT OCTET STRING OPTIONAL -- must have
-- should encapsulate DER of PKCS15Token
}

P15-AuthAttributes ::= SET SIZE (1..MAX) OF P15-Attribute
-- should contain:

-- 1) attrType = id-contentType:
-- { iso(1) member-body(2)  us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
-- attrValues - one OID - 1.2.840.113549.1.15.3.1

-- 2) attrType = id-messageDigest:
-- { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
-- attrValues - one OCTET STRING with hash

P15-Attribute ::= SEQUENCE {
     attrType OBJECT IDENTIFIER,
```

```
     attrValues SET OF P15-AttributeValue
}

P15-AttributeValue ::= ANY

P15-MessageAuthenticationCode ::= OCTET STRING
-- contains HMAC of re-encoded DER (EXPLICIT TAGS) of AuthAttributes



-----------------------------------------------------------------------------------------

P15-PKCS15Token ::= SEQUENCE {
       version               INTEGER {v1(0)}, -- should be 0
       keyManagementInfo     [0] P15-KeyManagementInfo OPTIONAL,
       pkcs15Objects         SEQUENCE OF P15-PKCS15Objects
}

P15-KeyManagementInfo ::= SEQUENCE OF P15-KeyManagementInfoElem

P15-KeyManagementInfoElem ::= SEQUENCE {
       keyId P15-Identifier,
       keyInfo CHOICE {
              recipientInfo P15-RecipientInfo, -- not used
              passwordInfo [0] P15-PasswordInfo
       }
} --(CONSTRAINED BY {  Each keyID must be unique })

P15-Identifier ::= OCTET STRING (SIZE (0..pkcs15-ub-identifier))

pkcs15-ub-identifier INTEGER ::= 255

P15-PasswordInfo ::= SEQUENCE {
       hint           P15-Label OPTIONAL,
       algId          P15-KeyDerivationAlgorithmIdentifier,
...
} --(CONSTRAINED BY {keyID shall point to a KEKRecipientInfo})

P15-Label ::= UTF8String (SIZE(0..pkcs15-ub-label))

pkcs15-ub-label       INTEGER ::= pkcs15-ub-identifier

P15-KeyDerivationAlgorithmIdentifier ::= P15-GostKeyDerivationAlgorithmIdentifier

P15-GostKeyDerivationAlgorithmIdentifier ::= SEQUENCE {
       algorithm      OBJECT IDENTIFIER,
-- must be {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-5(5) pbkdf2(12) }
       parameters     ANY OPTIONAL -- must be PBKDF2-params
}

P15-PBKDF2-params ::= SEQUENCE {
       salt    CHOICE {
               specified OCTET STRING,
                otherSource P15-AlgorithmIdentifier -- not used
       },
       iterationCount INTEGER (1..MAX),
       keyLength      INTEGER (1..MAX) OPTIONAL, -- must be 32
       prf            P15-HmacGostR3411Algorithm OPTIONAL -- must be present
}



P15-PKCS15Objects ::= CHOICE {
       privateKeys           [0] P15-PrivateKeys,
       publicKeys            [1] P15-PublicKeys,
       trustedPublicKeys     [2] P15-PublicKeys,   -- not used
       secretKeys            [3] P15-SecretKeys,   -- not yet
       certificates          [4] P15-Certificates,
       trustedCertificates   [5] P15-Certificates, -- root certificates
       usefulCertificates    [6] P15-Certificates, -- not used
       dataObjects           [7] P15-DataObjects,  -- random values, CRLs
       authObjects           [8] P15-AuthObjects,  -- not used
... -- For future extensions
}

P15-PrivateKeys ::= P15-PathOrObjectsPrivateKeyType

P15-PathOrObjectsPrivateKeyType ::= CHOICE {
```

```
        path            P15-Path, -- not used
        objectsk        [0] SEQUENCE OF P15-PrivateKeyType, -- use, keys encrypted in ObjectValue
        ...,
        indirect-protected [1] P15-ReferencedValue, -- not used
-- EnvelopedData {SEQUENCE OF ObjectType}}
        direct-protected [2] P15-EnvelopedData -- not used, we use ObjectValue encryption
}

P15-PrivateKeyType ::= CHOICE {
        privateRSAKey  P15-PrivateKeyObjectPrivateRSAKeyAttributes, -- not used
        privateECKey   [0] P15-PrivateKeyObjectPrivateECKeyAttributes, -- not used
        privateDHKey   [1] P15-PrivateKeyObjectPrivateDHKeyAttributes, -- not used
        privateDSAKey  [2] P15-PrivateKeyObjectPrivateDSAKeyAttributes,-- not used
        privateKEAKey  [3] P15-PrivateKeyObjectPrivateKEAKeyAttributes,-- not used
        privateGostR3410-2001Key      [26] P15-PKCS15ObjectPrivateKey, -- use
... -- For future extensions
}


--PKCS15Object {ClassAttributes, SubClassAttributes, TypeAttributes} ::= SEQUENCE {
--      commonObjectAttributesCommonObjectAttributes,
--      classAttributes               ClassAttributes,
--      subClassAttributes    [0] SubClassAttributes OPTIONAL,
--      typeAttributes        [1] TypeAttributes
--}

--PrivateKeyObject {KeyAttributes} ::= PKCS15Object {CommonKeyAttributes,
--      CommonPrivateKeyAttributes, KeyAttributes}

P15-PKCS15ObjectPrivateKey ::= SEQUENCE {
        commonObjectAttributesP15-CommonObjectAttributes,
        classAttributes               P15-CommonKeyAttributes,
        subClassAttributes    [0] P15-CommonPrivateKeyAttributes OPTIONAL,
        typeAttributes        [1] P15-PrivateGostKeyAttributes
}

P15-CommonObjectAttributes ::= SEQUENCE {
        label   P15-Label OPTIONAL, -- use for container names
        flags   P15-CommonObjectFlags OPTIONAL,
        authId  P15-Identifier OPTIONAL, -- not used
        ...,
        userConsent INTEGER  OPTIONAL, -- not used
        accessControlRules SEQUENCE SIZE (1..MAX) OF P15-AccessControlRule OPTIONAL -- not used
}

P15-CommonObjectFlags ::= BIT STRING {
        private         (0), -- set for private keys, random
        modifiable      (1)  -- set for random
}

P15-CommonKeyAttributes ::= SEQUENCE {
        iD              P15-Identifier, -- should be same as in certificate or in pubkey
        usage           P15-KeyUsageFlags,
        native          BOOLEAN DEFAULT TRUE,         -- not used
        accessFlags     P15-KeyAccessFlags OPTIONAL,  -- may be used
        keyReference    P15-Reference OPTIONAL,       -- not used
        startDate       GeneralizedTime OPTIONAL,     -- may be used
        endDate         [0] GeneralizedTime OPTIONAL, -- may be used
... -- For future extensions
}

P15-KeyUsageFlags ::= BIT STRING {
        encrypt         (0),
        decrypt         (1),
        sign            (2),
        signRecover     (3), -- not used
        wrap            (4),
        unwrap          (5),
        verify          (6),
        verifyRecover   (7), -- not used
        derive          (8),
        nonRepudiation (9)  -- not used
}

P15-KeyAccessFlags ::= BIT STRING {
        sensitive               (0),
        extractable             (1),
        alwaysSensitive                 (2),
        neverExtractable        (3),
```

```
       local                (4)
}

P15-CommonPrivateKeyAttributes ::= SEQUENCE {
       subjectName    P15-Name OPTIONAL, -- use
       keyIdentifiers [0] SEQUENCE OF P15-CredentialIdentifier  OPTIONAL, -- not used (yet)
{{KeyIdentifiers}}
... -- For future extensions
}

P15-Name ::= CHOICE {
       rdnSequence    P15-RDNSequence
}

P15-RDNSequence ::= SEQUENCE OF P15-RelativeDistinguishedName

P15-RelativeDistinguishedName ::= SET SIZE (1..MAX) OF P15-AttributeTypeAndValue

P15-AttributeTypeAndValue ::= SEQUENCE {
       type    P15-AttributeType,
       value   P15-AttributeValue
}

P15-AttributeType ::= OBJECT IDENTIFIER


P15-PrivateGostKeyAttributes ::= SEQUENCE {
       value          P15-ObjectValueGostPrivateKey,
       keyInfo        P15-KeyInfoPrivateGost  OPTIONAL, -- if absent - cproSetA
... -- For future extensions
}

--ObjectValue { Type } ::= CHOICE {
--      indirect              ReferencedValue {Type},
--      direct                [0] Type,
--      indirect-protected    [1] ReferencedValue {EnvelopedData {Type}},
--      direct-protected      [2] EnvelopedData {Type}
--}

P15-ObjectValueGostPrivateKey ::= CHOICE {
       indirect              P15-ReferencedValue, -- not used
       direct                [0] ANY, -- not used
       indirect-protected    [1] P15-ReferencedValue, -- not used
       direct-protected      [2] P15-EnvelopedData -- use (encapsulates GostPrivateKey)
}

P15-GostPrivateKey ::= P15-KeyValueMask

P15-KeyValueMask ::= OCTET STRING
-- must be ( Km | M1 | M2 | ... | Mk ) - little-endian


P15-EnvelopedData ::= SEQUENCE {
       version               P15-CMSVersion, -- should be 2
       originatorInfo        [0] IMPLICIT P15-OriginatorInfo OPTIONAL, -- not used
       recipientInfos        P15-RecipientInfos, -- contains only 1 KEKRecipientInfo
       encryptedContentInfo  P15-EncryptedContentInfo,
       unprotectedAttrs      [1] IMPLICIT P15-UnprotectedAttributes OPTIONAL -- not used
}


P15-EncryptedContentInfo ::= SEQUENCE {
       contentType           OBJECT IDENTIFIER,
-- must be { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1 }
       contentEncryptionAlgorithm P15-ContentEncryptionAlgorithmIdentifier,
       encryptedContent      [0] IMPLICIT P15-EncryptedContent OPTIONAL -- must have
}

P15-ContentEncryptionAlgorithmIdentifier ::= P15-GostEncryptionImitAlgorithmIdentifier

P15-GostEncryptionImitAlgorithmIdentifier ::= SEQUENCE {
       algorithm      OBJECT IDENTIFIER,
-- must be
-- iso(1) member-body(2) ru(643) rans(2) infotecs(4) ?(3) gost-28147(2) cbc-imm(2)
       parameters     ANY OPTIONAL -- but MUST be present and must be Gost28147-89-Parameters
}

P15-Gost28147-89-Parameters ::= SEQUENCE {
         iv                   P15-Gost28147-89-IV,
```

```
         encryptionParamSet   P15-Gost28147-89-ParamSet
}

P15-Gost28147-89-IV ::= OCTET STRING (SIZE (8))

P15-EncryptedContent ::= OCTET STRING -- Encrypted data + imit


--KeyInfo {ParameterType, OperationsType} ::= CHOICE {
--      reference      Reference,
--      paramsAndOps   SEQUENCE {
--             parameters            ParameterType,
--             supportedOperations   OperationsType OPTIONAL
--      }
--}

P15-KeyInfoPrivateGost ::= CHOICE {
       reference      P15-Reference, -- not used
       paramsAndOps   SEQUENCE {
              parameters            P15-KeyParameters,
              supportedOperations   P15-PublicKeyOperations OPTIONAL -- not used
       }
}

P15-KeyParameters ::= CHOICE {
       cryptoProParamSet     OBJECT IDENTIFIER, -- used
-- may be:
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-signs(35) cryptopro-A(1) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-signs(35) cryptopro-B(2) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-signs(35) cryptopro-C(3) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-exchanges(36) cryptopro-XchA(0) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-exchanges(36) cryptopro-XchB(1) }

       privateKeyParamSet    [0] P15-GostR3410-2001-PublicKeyParameters, -- recognized
       secretKeyParamSet     [1] P15-Gost28147-89-ParamSetParameters, -- not used
       ...
}

P15-GostR3410-2001-PublicKeyParameters ::= SEQUENCE {
       publicKeyParamSet     OBJECT IDENTIFIER,
-- may be:
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-signs(35) cryptopro-A(1) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-signs(35) cryptopro-B(2) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-signs(35) cryptopro-C(3) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-exchanges(36) cryptopro-XchA(0) }
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) ecc-exchanges(36) cryptopro-XchB(1) }

       digestParamSet        OBJECT IDENTIFIER,
-- must be:
-- { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) hashes(30) cryptopro(1) }

       encryptionParamSet    P15-Gost28147-89-ParamSet OPTIONAL
}

P15-Gost28147-89-ParamSetParameters ::= SEQUENCE {
        eUZ          P15-Gost28147-89-UZ,
        mode         INTEGER {
                         gost28147-89-CNT(0),
                         gost28147-89-CFB(1),
                         cryptoPro-CBC(2)
                     },
        shiftBits    INTEGER,
        keyMeshing   P15-AlgorithmIdentifier
}

P15-Gost28147-89-UZ ::= OCTET STRING (SIZE (64))

P15-PublicKeyOperations ::= P15-Operations

P15-Operations ::= BIT STRING {
       compute-checksum      (0), -- H/W computation of checksum
       compute-signature     (1), -- H/W computation of signature
       verify-checksum              (2), -- H/W verification of checksum
       verify-signature      (3), -- H/W verification of signature
       encipher              (4), -- H/W encryption of data
       decipher              (5), -- H/W decryption of data
       hash                  (6), -- H/W hashing
       generate-key          (7)  -- H/W key generation
}
```

```
P15-PublicKeys ::= P15-PathOrObjectsPublicKeyType

P15-PathOrObjectsPublicKeyType ::= CHOICE {
       path           P15-Path, -- not used
       objectspk      [0] SEQUENCE OF P15-PublicKeyType, -- use
       ...,
       indirect-protected [1] P15-ReferencedValue, -- not used
-- EnvelopedData {SEQUENCE OF ObjectType}}
       direct-protected [2] P15-EnvelopedData -- not used
}

P15-PublicKeyType ::= CHOICE {
       publicRSAKey   P15-PublicKeyObjectPublicRSAKeyAttributes,
       publicECKey    [0] P15-PublicKeyObjectPublicECKeyAttributes,
       publicDHKey    [1] P15-PublicKeyObjectPublicDHKeyAttributes,
       publicDSAKey   [2] P15-PublicKeyObjectPublicDSAKeyAttributes,
       publicKEAKey   [3] P15-PublicKeyObjectPublicKEAKeyAttributes,
       publicGostR3410-2001Key      [26] P15-PKCS15ObjectPublicKey, -- use
       ... -- For future extensions
}

P15-PKCS15ObjectPublicKey ::= SEQUENCE {
       commonObjectAttributesP15-CommonObjectAttributes,
       classAttributes              P15-CommonKeyAttributes,
       subClassAttributes    [0] P15-CommonPublicKeyAttributes OPTIONAL,
       typeAttributes        [1] P15-PublicGostKeyAttributes
}

P15-CommonPublicKeyAttributes ::= SEQUENCE {
       subjectName    P15-Name OPTIONAL, -- may use
       ...,
       trustedUsage   [0] P15-Usage OPTIONAL -- not used
}

P15-PublicGostKeyAttributes ::= SEQUENCE {
       value   P15-ObjectValueGostPublicKeyChoice,
       keyInfo P15-KeyInfoPublicGost OPTIONAL, -- may use
       ... -- For future extensions
}

P15-ObjectValueGostPublicKeyChoice ::= CHOICE {
       indirect              P15-ReferencedValue, -- not used
       direct                [0] P15-GostPublicKeyChoice,
       indirect-protected    [1] P15-ReferencedValue, -- not used
       direct-protected      [2] P15-EnvelopedData -- not used
}

P15-GostPublicKeyChoice ::= CHOICE {
       raw     P15-GostR3410-2001Point,
       spki    P15-SubjectPublicKeyInfo, -- not implemented yet
-- spki.algorithm.algorithm must be:
--  { iso(1) member-body(2) ru(643) rans(2) cryptopro(2) gostR3410-2001(19) }
-- spki.algorithm.parameters may be absent or must be P15-GostR3410-2001-PublicKeyParameters
-- spki.subjectPublicKey must encapsulate DER of OCTET STRING of 64-byte public key
       ...
}

P15-GostR3410-2001Point ::= OCTET STRING  -- {PubKeyX | PubKeyY} - little-endian

P15-KeyInfoPublicGost ::= CHOICE {
       reference      P15-Reference, -- not used
       paramsAndOpsPub       SEQUENCE {
              parameters            P15-KeyParameters,
              supportedOperations   P15-PublicKeyOperations OPTIONAL -- not used
       }
}




P15-Certificates ::= P15-PathOrObjectsCertificateType

P15-PathOrObjectsCertificateType ::= CHOICE {
       path           P15-Path, -- not used
       objectsc       [0] SEQUENCE OF P15-CertificateType, -- used
       ...,
```

```
        indirect-protected [1] P15-ReferencedValue, -- not used
-- EnvelopedData {SEQUENCE OF ObjectType}}
        direct-protected [2] P15-EnvelopedData -- not used
}

P15-CertificateType ::= CHOICE {
        x509Certificate       P15-PKCS15ObjectX509Certificate,

-- Other types not used
        x509AttributeCertificate [0] P15-CertificateObjectX509AttributeCertificateAttributes,
        pgpCertificate        [2] P15-CertificateObjectPGPCertificateAttributes,
        wtlsCertificate             [3] P15-CertificateObjectWTLSCertificateAttributes,
        x9-68Certificate      [4] P15-CertificateObjectX9-68CertificateAttributes,
        ...,
        cvCertificate         [5] P15-CertificateObjectCVCertificateAttributes
}

--CertificateObject {CertAttributes} ::= PKCS15Object
--      {CommonCertificateAttributes, NULL, CertAttributes}

P15-PKCS15ObjectX509Certificate ::= SEQUENCE {
        commonObjectAttributesP15-CommonObjectAttributes,
        classAttributes              P15-CommonCertificateAttributes,
        subClassAttributes    [0] NULL OPTIONAL,
        typeAttributes        [1] P15-X509CertificateAttributes
}

P15-CommonCertificateAttributes ::= SEQUENCE {
        iD             P15-Identifier, -- should be same as in private key
        authority      BOOLEAN DEFAULT FALSE, -- CA or end-user
        identifier     P15-CredentialIdentifier OPTIONAL, -- not used in software tokens
        certHash       [0] P15-OOBCertHash OPTIONAL, -- not used
        ...,
        trustedUsage   [1] P15-Usage OPTIONAL, -- not used (we use trustedCertificates)
        identifiers    [2] SEQUENCE OF P15-CredentialIdentifier OPTIONAL, -- not used (yet)
        implicitTrust  [3] BOOLEAN DEFAULT FALSE -- not used (we use trustedCertificates)
}

P15-X509CertificateAttributes ::= SEQUENCE {
        value          P15-ObjectValueCertificate,
        subject        P15-Name OPTIONAL, -- we use
        issuer         [0] P15-Name OPTIONAL, -- we use
        serialNumber   P15-CertificateSerialNumber OPTIONAL, -- we use
... -- For future extensions
}

P15-CertificateSerialNumber  ::=  INTEGER

P15-ObjectValueCertificate ::= CHOICE {
        indirect              P15-ReferencedValue, -- not used
        direct                [0] P15-Certificate, -- used
        indirect-protected    [1] P15-ReferencedValue, -- not used
        direct-protected      [2] P15-EnvelopedData -- not used
}

P15-Certificate ::= SEQUENCE  {
        tbsCertificate       P15-TBSCertificate,
        signatureAlgorithm   P15-AlgorithmIdentifier,
        signatureValue       BIT STRING
}

P15-TBSCertificate  ::=  SEQUENCE  {
         version         [0]  EXPLICIT P15-Version DEFAULT v1,
         serialNumber         P15-CertificateSerialNumber,
         signature            P15-AlgorithmIdentifier,
         issuer               P15-Name,
         validity             P15-Validity,
         subject              P15-Name,
         subjectPublicKeyInfo P15-SubjectPublicKeyInfo,
         issuerUniqueID  [1]  IMPLICIT P15-UniqueIdentifier OPTIONAL,
                              -- If present, version MUST be v2 or v3
         subjectUniqueID [2]  IMPLICIT P15-UniqueIdentifier OPTIONAL,
                              -- If present, version MUST be v2 or v3
         extensions      [3]  EXPLICIT P15-Extensions OPTIONAL
                              -- If present, version MUST be v3
}

P15-Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
```

```
P15-AlgorithmIdentifier  ::=  SEQUENCE  {
        algorithm               OBJECT IDENTIFIER,
        parameters              ANY OPTIONAL
}

P15-Validity ::= SEQUENCE {
        notBefore      P15-Time,
        notAfter       P15-Time
}

P15-Time ::= CHOICE {
        utcTime        UTCTime,
        generalTime    GeneralizedTime
}

P15-SubjectPublicKeyInfo  ::=  SEQUENCE  {
        algorithm            P15-AlgorithmIdentifier,
        subjectPublicKey     BIT STRING
}

P15-UniqueIdentifier  ::=  BIT STRING


P15-Extensions  ::=  SEQUENCE SIZE (1..MAX) OF P15-Extension

P15-Extension  ::=  SEQUENCE  {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING
}




P15-DataObjects ::= P15-PathOrObjectsDataType

P15-PathOrObjectsDataType ::= CHOICE {
       path           P15-Path, -- not used
       objectsd       [0] SEQUENCE OF P15-DataType, -- used for CRLs and random (encr)
       ...,
       indirect-protected [1] P15-ReferencedValue, -- not used
-- EnvelopedData {SEQUENCE OF ObjectType}}
       direct-protected [2] P15-EnvelopedData -- not used
}

P15-DataType ::= CHOICE {
       opaqueDO       P15-DataObjectOpaque,         -- not used
       externalIDO    [0] P15-DataObjectExternalIDO,       -- not used
       oidDO          [1] P15-PKCS15ObjectOidDO,
... -- For future extensions
}

--DataObjectOidDO {DataObjectAttributes} ::= PKCS15Object {
--      CommonDataObjectAttributes, NULL, OidDO}


P15-PKCS15ObjectOidDO ::= SEQUENCE {
       commonObjectAttributesP15-CommonObjectAttributes,
       classAttributes              P15-CommonDataObjectAttributes,
       subClassAttributes    [0] NULL OPTIONAL,
       typeAttributes        [1] P15-OidDO
}

P15-CommonDataObjectAttributes ::= SEQUENCE {
       applicationName              P15-Label OPTIONAL,   -- not used
       applicationOID        OBJECT IDENTIFIER OPTIONAL,
-- For FactorTSVersion:
-- {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) factor-
ts(13312) room503(503) content-types(1) factor-ts-version(3) }

-- For CRL:
-- {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) factor-
ts(13312) room503(503) content-types(1) x509crl(2) }

-- For random init value:
-- {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) factor-
ts(13312) room503(503) content-types(1) random-init(1) }
```

```
-- For abstract data identified by OID:
-- {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) factor-
ts(13312) room503(503) content-types(1) abstract-data(4) }


... -- For future extensions
} (WITH COMPONENTS {..., applicationName PRESENT}|WITH COMPONENTS {..., applicationOID PRESENT})

P15-OidDO ::= SEQUENCE {
       id     OBJECT IDENTIFIER, -- same as CommonDataObjectAttributes.applicationOID
       value   P15-ObjectValueAny
}

P15-ObjectValueAny ::= CHOICE {
       indirect              P15-ReferencedValue, -- not used
       direct                [0] ANY, -- CRLContainer, FactorTSVersion, FTSAbstractData
       indirect-protected    [1] P15-ReferencedValue, -- not used
       direct-protected      [2] P15-EnvelopedData -- RandomInitValue, FTSAbstractData
}

-- FTSAbstractData ::= OCTET STRING

P15-CRLContainer ::= SEQUENCE {
       iD     P15-Identifier, -- should be the same as issuer's certificate.
       issuer  [0] P15-Name OPTIONAL, -- we use
       crl    P15-CertificateList,
       ...
}

P15-CertificateList  ::=  SEQUENCE  {
        tbsCertList          P15-TBSCertList,
        signatureAlgorithm   P15-AlgorithmIdentifier,
        signatureValue       BIT STRING
}

P15-TBSCertList  ::=  SEQUENCE  {
        version                 P15-Version OPTIONAL,
                                     -- if present, MUST be v2
        signature               P15-AlgorithmIdentifier,
        issuer                  P15-Name,
        thisUpdate              P15-Time,
        nextUpdate              P15-Time OPTIONAL,
        revokedCertificates     SEQUENCE OF P15-CertListElem  OPTIONAL,
        crlExtensions           [0]  EXPLICIT P15-Extensions OPTIONAL
                                     -- if present, version MUST be v2
}

P15-CertListElem ::= SEQUENCE  {
       userCertificate         P15-CertificateSerialNumber,
       revocationDate          P15-Time,
       crlEntryExtensions      P15-Extensions OPTIONAL
        -- if present, version MUST be v2
}

P15-RandomInitValue ::= SEQUENCE {
       randomInit     OCTET STRING (SIZE (64)),
       moreRandom     OCTET STRING OPTIONAL,
       ...
}

P15-FactorTSVersion ::= SEQUENCE {
       majorVersion   INTEGER,
       minorVersion   [0] INTEGER OPTIONAL,
       ...
}

-------------------------------------------------------------------
-- Unused types --
-------------------------------------------------------------------


P15-OriginatorInfo ::= SEQUENCE {
        certs [0] IMPLICIT P15-CertificateSet OPTIONAL,
        crls [1] IMPLICIT P15-RevocationInfoChoices OPTIONAL
}

P15-CertificateSet ::= SET OF P15-CertificateChoices

P15-CertificateChoices ::= ANY
```

```
P15-RevocationInfoChoices ::= SET OF P15-RevocationInfoChoice

P15-RevocationInfoChoice ::= ANY


P15-UnauthAttributes ::= SET SIZE (1..MAX) OF P15-Attribute

P15-KeyTransRecipientInfo ::= SEQUENCE {
...
}
--     version CMSVersion,   always set to 0 or 2
--     rid RecipientIdentifier,
--     keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
--     encryptedKey EncryptedKey }


P15-KeyAgreeRecipientInfo ::= SEQUENCE {
       ...
}

P15-PasswordRecipientInfo ::= SEQUENCE {
       ...
}

P15-OtherRecipientInfo ::= SEQUENCE {
       ...
}

P15-OtherKeyAttribute ::= SEQUENCE { ... }

P15-SecretKeys ::= ANY

P15-AuthObjects ::= ANY

P15-Path ::= SEQUENCE { ... }

P15-ReferencedValue ::= CHOICE {
       path    P15-Path,
       url     P15-URL
}

P15-URL ::= CHOICE {
       url            PrintableString,
       urlWithDigest  [3] SEQUENCE {
              url     IA5String,
              digest  P15-DigestInfoWithDefault
       }
}

P15-DigestInfoWithDefault ::= SEQUENCE { ... }

P15-UnprotectedAttributes ::= SET SIZE (1..MAX) OF P15-Attribute

P15-PrivateKeyObjectPrivateRSAKeyAttributes ::= SEQUENCE { ... }

P15-PrivateKeyObjectPrivateECKeyAttributes ::= SEQUENCE { ... }

P15-PrivateKeyObjectPrivateDHKeyAttributes ::= SEQUENCE { ... }

P15-PrivateKeyObjectPrivateDSAKeyAttributes ::= SEQUENCE { ... }

P15-PrivateKeyObjectPrivateKEAKeyAttributes ::= SEQUENCE { ... }

P15-AccessControlRule ::= ANY


P15-Reference ::= INTEGER (0..pkcs15-ub-reference)

pkcs15-ub-reference   INTEGER ::= 255

P15-CredentialIdentifier ::= SEQUENCE { ... }

P15-CertificateObjectX509AttributeCertificateAttributes ::= SEQUENCE { ... }

P15-CertificateObjectPGPCertificateAttributes ::= SEQUENCE { ... }

P15-CertificateObjectWTLSCertificateAttributes ::= SEQUENCE { ... }
```

```
P15-CertificateObjectX9-68CertificateAttributes ::= SEQUENCE { ... }

P15-CertificateObjectCVCertificateAttributes ::= SEQUENCE { ... }

P15-OOBCertHash ::= SEQUENCE { ... }

P15-Usage ::= SEQUENCE { ... }

P15-DataObjectOpaque ::= SEQUENCE { ... }

P15-DataObjectExternalIDO ::= SEQUENCE { ... }

P15-PublicKeyObjectPublicRSAKeyAttributes ::= SEQUENCE { ... }

P15-PublicKeyObjectPublicECKeyAttributes ::= SEQUENCE { ... }

P15-PublicKeyObjectPublicDHKeyAttributes ::= SEQUENCE { ... }

P15-PublicKeyObjectPublicDSAKeyAttributes ::= SEQUENCE { ... }

P15-PublicKeyObjectPublicKEAKeyAttributes ::= SEQUENCE { ... }


END
```

Представление ASN:

```
  0 5404: SEQUENCE {
  4    1:  INTEGER 0
  7   89:  SET {
  9   87:   [2] {
 11    1:    INTEGER 4
 14    6:    SEQUENCE {
 16    4:     OCTET STRING 00 00 00 04
       :      }
 22   30:    SEQUENCE {
 24    7:     OBJECT IDENTIFIER '1 2 643 2 2 13 1'
 33   19:     SEQUENCE {
 35    7:      OBJECT IDENTIFIER
       :       id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2 31 1)
 44    8:      OCTET STRING 74 BA EE A0 BE CB 77 5E
       :       }
       :      }
 54   42:    OCTET STRING, encapsulates {
 56   40:     SEQUENCE {
 58   32:      OCTET STRING
       :       5E B1 D1 B6 42 1A 02 DE 0B C6 FC 8C 3E 8D 81 0D
       :       DF 8D 44 08 5D 54 EF 7E A2 77 6E 19 DA 3E 78 A1
 92    4:      OCTET STRING 39 93 A8 0D
       :       }
       :      }
       :     }
       :    }
 98    8:  SEQUENCE {
100    6:   OBJECT IDENTIFIER '1 2 643 2 2 10'
       :    }
108    8:  [1] {
110    6:   OBJECT IDENTIFIER GOST R 34.11-94 (1 2 643 2 2 9) (1 2 643 2 2 9)
       :    }
118 5174:  SEQUENCE {
122   10:   OBJECT IDENTIFIER
       :    pkcs15content (1 2 840 113549 1 15 3 1) (1 2 840 113549 1 15 3 1)
134 5158:   [0] {
138 5154:    OCTET STRING, encapsulates {
142 5150:     SEQUENCE {
146    1:      INTEGER 0
149   76:      [0] {
151   74:       SEQUENCE {
153    4:        OCTET STRING 00 00 00 04
159   66:        [0] {
161   64:         SEQUENCE {
163    9:          OBJECT IDENTIFIER
       :           pkcs5PBKDF2 (1 2 840 113549 1 5 12) (1 2 840 113549 1 5 12)
174   51:          SEQUENCE {
176   32:           OCTET STRING
```

```
        :          F4 53 80 45 B0 2F C8 C6 DE AA 01 ED A5 16 21 DD
        :          B1 65 FB 1F 53 AB C9 4C 1D 64 B3 BD 3F D9 D8 0C
 210    2:           INTEGER 2000
 214    1:           INTEGER 32
 217    8:           SEQUENCE {
 219    6:            OBJECT IDENTIFIER '1 2 643 2 2 10'
        :             }
        :            }
        :           }
        :          }
        :         }
        :        }
 227 5065:      SEQUENCE {
 231  365:       [7] {
 235  361:        [0] {
 239   64:         [1] {
 241   22:          SEQUENCE {
 243   17:           UTF8String 'Factor-TS version'
 262    1:           BIT STRING
        :            }
 265   13:          SEQUENCE {
 267   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 3'
        :            }
 280   23:          [1] {
 282   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 3'
 295    8:           [0] {
 297    6:            SEQUENCE {
 299    1:             INTEGER 2
 302    1:             [0] 00
        :              }
        :             }
        :            }
        :           }
 305  291:         [1] {
 309   23:          SEQUENCE {
 311   17:           UTF8String 'Random Init Value'
 330    2:           BIT STRING 6 unused bits
        :             '11'B
        :            }
 334   13:          SEQUENCE {
 336   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 1'
        :            }
 349  248:          [1] {
 352   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 1'
 365  232:           [2] {
 368    1:            INTEGER 2
 371   89:            SET {
 373   87:             [2] {
 375    1:              INTEGER 4
 378    6:              SEQUENCE {
 380    4:               OCTET STRING 00 00 00 04
        :               }
 386   30:              SEQUENCE {
 388    7:               OBJECT IDENTIFIER '1 2 643 2 2 13 1'
 397   19:               SEQUENCE {
 399    7:                OBJECT IDENTIFIER
        :                 id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2
31 1)
 408    8:                OCTET STRING 74 70 70 52 12 2A 80 50
        :                 }
        :                }
 418   42:              OCTET STRING, encapsulates {
 420   40:               SEQUENCE {
 422   32:                OCTET STRING
        :           5D 7F 85 0F 18 0A 20 A5 FA 27 BC D4 13 77 39 AF
        :           A3 51 DB E7 3C B3 88 80 BB BE B8 41 5B 42 46 28
 456    4:                 OCTET STRING 5A 69 79 CD
        :                  }
        :                 }
        :                }
        :               }
 462  135:             SEQUENCE {
 465    9:              OBJECT IDENTIFIER
        :               data (1 2 840 113549 1 7 1) (1 2 840 113549 1 7 1)
 476   31:              SEQUENCE {
 478    8:               OBJECT IDENTIFIER '1 2 643 2 4 3 2 2'
 488   19:               SEQUENCE {
 490    8:                OCTET STRING DD 8E C8 00 0F CA 11 88
 500    7:                OBJECT IDENTIFIER
```

```
        :                id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2 31
1)
        :                }
        :               }
 509   89:             [0]
        :           93 9B 98 38 70 4A 73 DD A0 AE AF 87 4C 4A 00 AD
        :           62 B8 21 AA 5C 89 C2 FF 92 1C 5C 43 40 54 BC B6
        :           AA 28 D3 14 8B E9 6F 62 F2 06 37 69 25 2C 5D 09
        :           C9 26 44 14 23 51 85 DD 99 06 95 02 8E 0B 98 BE
        :           F5 46 55 CF 63 D8 E5 48 7D 63 25 75 2B F4 B1 93
        :           E6 3E 22 AA DB DC 46 03 91
        :            }
        :           }
        :          }
        :         }
        :        }
 600 1021:       [5] {
 604 1017:        [0] {
 608 1013:         SEQUENCE {
 612   27:          SEQUENCE {
 614   22:           UTF8String 'Root Certificate of CA'
 638    1:           BIT STRING
        :            }
 641    9:          SEQUENCE {
 643    4:           OCTET STRING 00 00 00 01
 649    1:           BOOLEAN TRUE
        :            }
 652  969:          [1] {
 656  697:           [0] {
 660  616:            SEQUENCE {
 664    3:             [0] {
 666    1:              INTEGER 2
        :              }
 669   16:             INTEGER
        :           07 48 BA C5 90 EA C5 9B 4C 4F 0F E7 04 98 9C A8
 687    8:             SEQUENCE {
 689    6:              OBJECT IDENTIFIER
        :               GOST R 34.11/34.10-2001 (1 2 643 2 2 3) (1 2 643 2 2 3)
        :               }
 697  122:             SEQUENCE {
 699   35:              SET {
 701   33:               SEQUENCE {
 703    9:                OBJECT IDENTIFIER
        :                 emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
 714   20:                IA5String 'mivanov@factor-ts.ru'
        :                 }
        :                }
 736   11:              SET {
 738    9:               SEQUENCE {
 740    3:                OBJECT IDENTIFIER
        :                 countryName (2 5 4 6) (2 5 4 6)
 745    2:                PrintableString 'RU'
        :                 }
        :                }
 749   15:              SET {
 751   13:               SEQUENCE {
 753    3:                OBJECT IDENTIFIER
        :                 localityName (2 5 4 7) (2 5 4 7)
 758    6:                PrintableString 'Moscow'
        :                 }
        :                }
 766   18:              SET {
 768   16:               SEQUENCE {
 770    3:                OBJECT IDENTIFIER
        :                 organizationName (2 5 4 10) (2 5 4 10)
 775    9:                PrintableString 'CryptoPro'
        :                 }
        :                }
 786   14:              SET {
 788   12:               SEQUENCE {
 790    3:                OBJECT IDENTIFIER
        :                 organizationalUnitName (2 5 4 11) (2 5 4 11)
 795    5:                PrintableString 'Promo'
        :                 }
        :                }
 802   17:              SET {
 804   15:               SEQUENCE {
 806    3:                OBJECT IDENTIFIER
```

```
        :                commonName (2 5 4 3) (2 5 4 3)
 811    8:               PrintableString 'Maxim UC'
        :                }
        :               }
        :              }
 821   30:             SEQUENCE {
 823   13:              UTCTime 21/03/2012 12:39:38 GMT
 838   13:              UTCTime 21/03/2017 12:46:12 GMT
        :              }
 853  122:             SEQUENCE {
 855   35:              SET {
 857   33:               SEQUENCE {
 859    9:                OBJECT IDENTIFIER
        :                 emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
 870   20:               IA5String 'mivanov@factor-ts.ru'
        :                }
        :               }
 892   11:              SET {
 894    9:               SEQUENCE {
 896    3:                OBJECT IDENTIFIER
        :                 countryName (2 5 4 6) (2 5 4 6)
 901    2:               PrintableString 'RU'
        :                }
        :               }
 905   15:              SET {
 907   13:               SEQUENCE {
 909    3:                OBJECT IDENTIFIER
        :                 localityName (2 5 4 7) (2 5 4 7)
 914    6:               PrintableString 'Moscow'
        :                }
        :               }
 922   18:              SET {
 924   16:               SEQUENCE {
 926    3:                OBJECT IDENTIFIER
        :                 organizationName (2 5 4 10) (2 5 4 10)
 931    9:               PrintableString 'CryptoPro'
        :                }
        :               }
 942   14:              SET {
 944   12:               SEQUENCE {
 946    3:                OBJECT IDENTIFIER
        :                 organizationalUnitName (2 5 4 11) (2 5 4 11)
 951    5:               PrintableString 'Promo'
        :                }
        :               }
 958   17:              SET {
 960   15:               SEQUENCE {
 962    3:                OBJECT IDENTIFIER
        :                 commonName (2 5 4 3) (2 5 4 3)
 967    8:               PrintableString 'Maxim UC'
        :                }
        :               }
        :              }
 977   99:             SEQUENCE {
 979   28:              SEQUENCE {
 981    6:               OBJECT IDENTIFIER
        :                GOST R 34.10-2001 (1 2 643 2 2 19) (1 2 643 2 2 19)
 989   18:              SEQUENCE {
 991    7:               OBJECT IDENTIFIER
        :                id-GostR3410-2001-CryptoPro-A-ParamSet (1 2 643 2 2 35 1) (1 2 643 2 2
35 1)
1000    7:               OBJECT IDENTIFIER
        :                id-GostR3411-94-CryptoProParamSet (1 2 643 2 2 30 1) (1 2 643 2 2 30
1)
        :                }
        :               }
1009   67:              BIT STRING, encapsulates {
1012   64:               OCTET STRING
        :          97 CB DD 42 DF 80 28 13 B2 99 11 64 6B E1 38 12
        :          02 1F 6E 83 5F B3 35 B1 48 15 E0 43 CD 76 24 6D
        :          8D 70 52 10 B8 61 47 40 CF E2 31 4E 54 51 39 D5
        :          CF 23 BB 24 47 59 27 2F D7 9D F4 42 A8 C4 DD 9C
        :               }
        :              }
1078  199:             [3] {
1081  196:              SEQUENCE {
1084   11:               SEQUENCE {
1086    3:                OBJECT IDENTIFIER
        :                 keyUsage (2 5 29 15) (2 5 29 15)
```

```
1091    4:               OCTET STRING, encapsulates {
1093    2:                BIT STRING 1 unused bit
        :                  '1000011'B
        :                 }
        :                }
1097   15:              SEQUENCE {
1099    3:               OBJECT IDENTIFIER
        :                basicConstraints (2 5 29 19) (2 5 29 19)
1104    1:               BOOLEAN TRUE
1107    5:               OCTET STRING, encapsulates {
1109    3:                SEQUENCE {
1111    1:                 BOOLEAN TRUE
        :                 }
        :                }
        :               }
1114   29:              SEQUENCE {
1116    3:               OBJECT IDENTIFIER
        :                subjectKeyIdentifier (2 5 29 14) (2 5 29 14)
1121   22:               OCTET STRING, encapsulates {
1123   20:                OCTET STRING
        :          C3 99 AC 2E F8 F6 FC F0 62 2C 8A 80 35 DF DA 63
        :          28 17 EF ED
        :                }
        :               }
1145  115:              SEQUENCE {
1147    3:               OBJECT IDENTIFIER
        :                cRLDistributionPoints (2 5 29 31) (2 5 29 31)
1152  108:               OCTET STRING, encapsulates {
1154  106:                SEQUENCE {
1156  104:                 SEQUENCE {
1158  102:                  [0] {
1160  100:                   [0] {
1162   48:                    [6]
        :          'http://voenmeh-d0f286a/CertEnroll/Maxim%20UC.crl'
1212   48:                    [6]
        :          'file://\\voenmeh-d0f286a\CertEnroll\Maxim UC.crl'
        :                   }
        :                  }
        :                 }
        :                }
        :               }
        :              }
1262   16:              SEQUENCE {
1264    9:               OBJECT IDENTIFIER
        :                cAKeyCertIndexPair (1 3 6 1 4 1 311 21 1) (1 3 6 1 4 1 311 21 1)
1275    3:               OCTET STRING, encapsulates {
1277    1:                INTEGER 0
        :                 }
        :                }
        :               }
        :              }
        :             }
1280    8:            SEQUENCE {
1282    6:             OBJECT IDENTIFIER
        :              GOST R 34.11/34.10-2001 (1 2 643 2 2 3) (1 2 643 2 2 3)
        :              }
1290   65:            BIT STRING
        :          C1 74 E0 FC 28 6F 84 9C BA FA 24 ED A3 AB D1 44
        :          97 D4 E2 46 74 C2 D4 9E B9 F8 1B 53 1C 98 BA AA
        :          95 DB EB DA 76 A2 45 2F 05 99 F1 96 B3 9F 2F F1
        :          71 E5 12 66 CB EB 59 39 32 F5 7B 6A D0 7C F8 AD
        :             }
1357  122:           SEQUENCE {
1359   35:            SET {
1361   33:             SEQUENCE {
1363    9:              OBJECT IDENTIFIER
        :               emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
1374   20:              IA5String 'mivanov@factor-ts.ru'
        :               }
        :              }
1396   11:            SET {
1398    9:             SEQUENCE {
1400    3:              OBJECT IDENTIFIER
        :               countryName (2 5 4 6) (2 5 4 6)
1405    2:              PrintableString 'RU'
        :               }
        :              }
1409   15:            SET {
1411   13:             SEQUENCE {
```

```
1413    3:              OBJECT IDENTIFIER
        :               localityName (2 5 4 7) (2 5 4 7)
1418    6:              PrintableString 'Moscow'
        :               }
        :              }
1426   18:             SET {
1428   16:              SEQUENCE {
1430    3:               OBJECT IDENTIFIER
        :                organizationName (2 5 4 10) (2 5 4 10)
1435    9:               PrintableString 'CryptoPro'
        :               }
        :              }
1446   14:             SET {
1448   12:              SEQUENCE {
1450    3:               OBJECT IDENTIFIER
        :                organizationalUnitName (2 5 4 11) (2 5 4 11)
1455    5:               PrintableString 'Promo'
        :               }
        :              }
1462   17:             SET {
1464   15:              SEQUENCE {
1466    3:               OBJECT IDENTIFIER
        :                commonName (2 5 4 3) (2 5 4 3)
1471    8:               PrintableString 'Maxim UC'
        :               }
        :              }
        :             }
1481  124:            [0] {
1483  122:             SEQUENCE {
1485   35:              SET {
1487   33:               SEQUENCE {
1489    9:                OBJECT IDENTIFIER
        :                 emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
1500   20:                IA5String 'mivanov@factor-ts.ru'
        :                }
        :               }
1522   11:              SET {
1524    9:               SEQUENCE {
1526    3:                OBJECT IDENTIFIER
        :                 countryName (2 5 4 6) (2 5 4 6)
1531    2:                PrintableString 'RU'
        :                }
        :               }
1535   15:              SET {
1537   13:               SEQUENCE {
1539    3:                OBJECT IDENTIFIER
        :                 localityName (2 5 4 7) (2 5 4 7)
1544    6:                PrintableString 'Moscow'
        :                }
        :               }
1552   18:              SET {
1554   16:               SEQUENCE {
1556    3:                OBJECT IDENTIFIER
        :                 organizationName (2 5 4 10) (2 5 4 10)
1561    9:                PrintableString 'CryptoPro'
        :                }
        :               }
1572   14:              SET {
1574   12:               SEQUENCE {
1576    3:                OBJECT IDENTIFIER
        :                 organizationalUnitName (2 5 4 11) (2 5 4 11)
1581    5:                PrintableString 'Promo'
        :                }
        :               }
1588   17:              SET {
1590   15:               SEQUENCE {
1592    3:                OBJECT IDENTIFIER
        :                 commonName (2 5 4 3) (2 5 4 3)
1597    8:                PrintableString 'Maxim UC'
        :                }
        :               }
        :              }
        :             }
1607   16:            INTEGER
        :           07 48 BA C5 90 EA C5 9B 4C 4F 0F E7 04 98 9C A8
        :             }
        :            }
        :           }
        :          }
```

```
1625  888:       [7] {
1629  884:        [0] {
1633  880:         [1] {
1637   16:          SEQUENCE {
1639   11:           UTF8String 'CRL from CA'
1652    1:           BIT STRING
         :            }
1655   13:          SEQUENCE {
1657   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 2'
         :            }
1670  843:          [1] {
1674   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 2'
1687  826:           [0] {
1691  822:            SEQUENCE {
1695    4:             OCTET STRING 00 00 00 01
1701  124:             [0] {
1703  122:              SEQUENCE {
1705   35:               SET {
1707   33:                SEQUENCE {
1709    9:                 OBJECT IDENTIFIER
         :                  emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
1720   20:                 IA5String 'mivanov@factor-ts.ru'
         :                  }
         :                 }
1742   11:               SET {
1744    9:                SEQUENCE {
1746    3:                 OBJECT IDENTIFIER
         :                  countryName (2 5 4 6) (2 5 4 6)
1751    2:                 PrintableString 'RU'
         :                  }
         :                 }
1755   15:               SET {
1757   13:                SEQUENCE {
1759    3:                 OBJECT IDENTIFIER
         :                  localityName (2 5 4 7) (2 5 4 7)
1764    6:                 PrintableString 'Moscow'
         :                  }
         :                 }
1772   18:               SET {
1774   16:                SEQUENCE {
1776    3:                 OBJECT IDENTIFIER
         :                  organizationName (2 5 4 10) (2 5 4 10)
1781    9:                 PrintableString 'CryptoPro'
         :                  }
         :                 }
1792   14:               SET {
1794   12:                SEQUENCE {
1796    3:                 OBJECT IDENTIFIER
         :                  organizationalUnitName (2 5 4 11) (2 5 4 11)
1801    5:                 PrintableString 'Promo'
         :                  }
         :                 }
1808   17:               SET {
1810   15:                SEQUENCE {
1812    3:                 OBJECT IDENTIFIER
         :                  commonName (2 5 4 3) (2 5 4 3)
1817    8:                 PrintableString 'Maxim UC'
         :                  }
         :                 }
         :                }
         :               }
1827  686:              SEQUENCE {
1831  605:               SEQUENCE {
1835    1:                INTEGER 1
1838    8:                SEQUENCE {
1840    6:                 OBJECT IDENTIFIER
         :                  GOST R 34.11/34.10-2001 (1 2 643 2 2 3) (1 2 643 2 2 3)
         :                 }
1848  122:                SEQUENCE {
1850   35:                 SET {
1852   33:                  SEQUENCE {
1854    9:                   OBJECT IDENTIFIER
         :                    emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
1865   20:                   IA5String 'mivanov@factor-ts.ru'
         :                    }
         :                   }
1887   11:                 SET {
1889    9:                  SEQUENCE {
1891    3:                   OBJECT IDENTIFIER
```

```
         :                   countryName (2 5 4 6) (2 5 4 6)
1896     2:                  PrintableString 'RU'
         :                   }
         :                  }
1900    15:                SET {
1902    13:                 SEQUENCE {
1904     3:                  OBJECT IDENTIFIER
         :                   localityName (2 5 4 7) (2 5 4 7)
1909     6:                  PrintableString 'Moscow'
         :                   }
         :                  }
1917    18:                SET {
1919    16:                 SEQUENCE {
1921     3:                  OBJECT IDENTIFIER
         :                   organizationName (2 5 4 10) (2 5 4 10)
1926     9:                  PrintableString 'CryptoPro'
         :                   }
         :                  }
1937    14:                SET {
1939    12:                 SEQUENCE {
1941     3:                  OBJECT IDENTIFIER
         :                   organizationalUnitName (2 5 4 11) (2 5 4 11)
1946     5:                  PrintableString 'Promo'
         :                   }
         :                  }
1953    17:                SET {
1955    15:                 SEQUENCE {
1957     3:                  OBJECT IDENTIFIER
         :                   commonName (2 5 4 3) (2 5 4 3)
1962     8:                  PrintableString 'Maxim UC'
         :                   }
         :                  }
         :                 }
1972    13:               UTCTime 15/05/2012 09:10:06 GMT
1987    13:               UTCTime 22/05/2012 21:30:06 GMT
2002   129:               SEQUENCE {
2005    41:                SEQUENCE {
2007    10:                 INTEGER
         :           61 04 D6 67 00 00 00 00 00 12
2019    13:                 UTCTime 02/05/2012 11:41:27 GMT
2034    12:                 SEQUENCE {
2036    10:                  SEQUENCE {
2038     3:                   OBJECT IDENTIFIER
         :                    cRLReason (2 5 29 21) (2 5 29 21)
2043     3:                   OCTET STRING, encapsulates {
2045     1:                    ENUMERATED 5
         :                    }
         :                   }
         :                  }
         :                 }
2048    41:                SEQUENCE {
2050    10:                 INTEGER
         :           61 10 5F A6 00 00 00 00 00 07
2062    13:                 UTCTime 02/05/2012 11:38:20 GMT
2077    12:                 SEQUENCE {
2079    10:                  SEQUENCE {
2081     3:                   OBJECT IDENTIFIER
         :                    cRLReason (2 5 29 21) (2 5 29 21)
2086     3:                   OCTET STRING, encapsulates {
2088     1:                    ENUMERATED 5
         :                    }
         :                   }
         :                  }
         :                 }
2091    41:                SEQUENCE {
2093    10:                 INTEGER
         :           61 E9 42 A9 00 00 00 00 00 11
2105    13:                 UTCTime 02/05/2012 11:38:05 GMT
2120    12:                 SEQUENCE {
2122    10:                  SEQUENCE {
2124     3:                   OBJECT IDENTIFIER
         :                    cRLReason (2 5 29 21) (2 5 29 21)
2129     3:                   OCTET STRING, encapsulates {
2131     1:                    ENUMERATED 5
         :                    }
         :                   }
         :                  }
         :                 }
         :                }
```

```
2134  302:              [0] {
2138  298:               SEQUENCE {
2142   31:                SEQUENCE {
2144    3:                 OBJECT IDENTIFIER
        :                  authorityKeyIdentifier (2 5 29 35) (2 5 29 35)
2149   24:                 OCTET STRING, encapsulates {
2151   22:                  SEQUENCE {
2153   20:                   [0]
        :          C3 99 AC 2E F8 F6 FC F0 62 2C 8A 80 35 DF DA 63
        :          28 17 EF ED
        :                   }
        :                  }
        :                 }
2175   16:                SEQUENCE {
2177    9:                 OBJECT IDENTIFIER
        :                  cAKeyCertIndexPair (1 3 6 1 4 1 311 21 1) (1 3 6 1 4 1 311 21 1)
2188    3:                 OCTET STRING, encapsulates {
2190    1:                  INTEGER 0
        :                  }
        :                 }
2193   10:                SEQUENCE {
2195    3:                 OBJECT IDENTIFIER
        :                  cRLNumber (2 5 29 20) (2 5 29 20)
2200    3:                 OCTET STRING, encapsulates {
2202    1:                  INTEGER 5
        :                  }
        :                 }
2205   28:                SEQUENCE {
2207    9:                 OBJECT IDENTIFIER '1 3 6 1 4 1 311 21 4'
2218   15:                 OCTET STRING, encapsulates {
2220   13:                  UTCTime 22/05/2012 09:20:06 GMT
        :                  }
        :                 }
2235  202:                SEQUENCE {
2238    9:                 OBJECT IDENTIFIER '1 3 6 1 4 1 311 21 14'
2249  188:                 OCTET STRING, encapsulates {
2252  185:                  SEQUENCE {
2255  182:                   SEQUENCE {
2258  179:                    [0] {
2261  176:                     [0] {
2264  173:                      [6]
        :          'ldap:///CN=Maxim%20UC,CN=voenmeh-d0f286a,CN=CDP,'
        :          'CN=Public%20Key%20Services,CN=Services,DC=Unavai'
        :          'lableConfigDN?certificateRevocationList?base?obj'
        :          'ectClass=cRLDistributionPoint'
        :                     }
        :                    }
        :                   }
        :                  }
        :                 }
        :                }
        :               }
2440    8:              SEQUENCE {
2442    6:               OBJECT IDENTIFIER
        :                GOST R 34.11/34.10-2001 (1 2 643 2 2 3) (1 2 643 2 2 3)
        :                }
2450   65:              BIT STRING
        :          70 B6 42 8A 9A E3 05 82 9E 7F 5B 97 A1 6A B1 84
        :          FB F8 23 E7 F2 CD 02 A3 02 92 E8 53 83 8F 51 F4
        :          88 A4 0C 37 C6 9D 3C 4B AB 0C 3A A1 0C 0B 7F 02
        :          35 02 77 88 D2 A3 04 FD 67 EC 9B 92 B0 83 AB 57
        :               }
        :              }
        :             }
        :            }
        :           }
        :          }
2517  551:        [0] {
2521  547:         [0] {
2525  543:          [26] {
2529   35:           SEQUENCE {
2531   29:            UTF8String 'Private Key of Andrey Fedotov'
2562    2:            BIT STRING 7 unused bits
        :             '1'B (bit 0)
        :             }
2566   49:           SEQUENCE {
```

```
2568    4:           OCTET STRING 00 00 00 02
2574    3:           BIT STRING 6 unused bits
         :            '0110010001'B
2579    2:           BIT STRING 5 unused bits
         :            '111'B
2583   15:           GeneralizedTime 18/05/2012 11:03:00 GMT
2600   15:           [0] 18/05/2013 11:12:00 GMT
         :            }
2617  189:          [0] {
2620  186:           SEQUENCE {
2623   35:            SET {
2625   33:             SEQUENCE {
2627    9:              OBJECT IDENTIFIER
         :               emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
2638   20:              IA5String 'fedotov@factor-ts.ru'
         :               }
         :              }
2660   11:            SET {
2662    9:             SEQUENCE {
2664    3:              OBJECT IDENTIFIER
         :               countryName (2 5 4 6) (2 5 4 6)
2669    2:              PrintableString 'RU'
         :               }
         :              }
2673   21:            SET {
2675   19:             SEQUENCE {
2677    3:              OBJECT IDENTIFIER
         :               localityName (2 5 4 7) (2 5 4 7)
2682   12:              BMPString '...>.A.:.2.0'
         :               }
         :              }
2696   27:            SET {
2698   25:             SEQUENCE {
2700    3:              OBJECT IDENTIFIER
         :               organizationName (2 5 4 10) (2 5 4 10)
2705   18:              BMPString '.$.0.:.B.>.@-.".!'
         :               }
         :              }
2725   17:            SET {
2727   15:             SEQUENCE {
2729    3:              OBJECT IDENTIFIER
         :               organizationalUnitName (2 5 4 11) (2 5 4 11)
2734    8:              BMPString '."5.A.B'
         :               }
         :              }
2744   63:            SET {
2746   61:             SEQUENCE {
2748    3:              OBJECT IDENTIFIER
         :               commonName (2 5 4 3) (2 5 4 3)
2753   54:              BMPString
         :          '.$.5.4.>.B.>.2 ...=.4.@.5.9 ...;.0.4.8.<.8.@.>.2'
         :          '.8.G'
         :               }
         :              }
         :             }
         :            }
2809  259:          [1] {
2813  245:           [2] {
2816    1:            INTEGER 2
2819   89:            SET {
2821   87:             [2] {
2823    1:              INTEGER 4
2826    6:              SEQUENCE {
2828    4:               OCTET STRING 00 00 00 04
         :                }
2834   30:              SEQUENCE {
2836    7:               OBJECT IDENTIFIER '1 2 643 2 2 13 1'
2845   19:               SEQUENCE {
2847    7:                OBJECT IDENTIFIER
         :                 id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2
31 1)
2856    8:                OCTET STRING 3F 3B F8 A1 0D 7F B6 83
         :                 }
         :                }
2866   42:              OCTET STRING, encapsulates {
2868   40:               SEQUENCE {
2870   32:                OCTET STRING
         :          10 A8 84 C3 2C 16 2F 2F 3E 46 97 D5 45 70 0D 6D
         :          83 AE A3 CB 56 55 D0 C3 75 16 C2 54 2C DA 21 56
```

```
2904    4:               OCTET STRING 37 08 3E 6D
        :                }
        :               }
        :              }
        :             }
2910  148:            SEQUENCE {
2913    9:             OBJECT IDENTIFIER
        :              data (1 2 840 113549 1 7 1) (1 2 840 113549 1 7 1)
2924   31:             SEQUENCE {
2926    8:              OBJECT IDENTIFIER '1 2 643 2 4 3 2 2'
2936   19:              SEQUENCE {
2938    8:               OCTET STRING A3 32 60 BC E4 20 74 30
2948    7:               OBJECT IDENTIFIER
        :                id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2 31
1)
        :               }
        :              }
2957  102:             [0]
        :            F7 F0 41 FC C5 14 CB 6D 2A EF A2 5E D2 D3 17 15
        :            DB 96 9B 62 F6 50 20 82 2D 1A 1E AE CE 3F E4 6F
        :            41 96 66 68 44 9F B5 A2 98 8F BC AE 61 86 B9 FD
        :            DF F9 81 33 47 08 32 20 0F 7B 4E 18 A0 0C DD 72
        :            A9 D2 E8 1E BB 8A 41 0B 88 EB A8 87 6B 4E 3D 0D
        :            46 B2 37 4A 65 00 6D 82 0A D5 52 F3 DA BB 4B 19
        :            09 5E DB 60 F8 CE
        :             }
        :            }
3061    9:           SEQUENCE {
3063    7:            OBJECT IDENTIFIER
        :             id-GostR3410-2001-CryptoPro-A-ParamSet (1 2 643 2 2 35 1) (1 2 643 2 2 35
1)
        :            }
        :           }
        :          }
        :         }
        :        }
3072 1346:       [4] {
3076 1342:        [0] {
3080 1338:         SEQUENCE {
3084   34:          SEQUENCE {
3086   29:           UTF8String 'Certificate of Andrey Fedotov'
3117    1:           BIT STRING
        :            }
3120    6:          SEQUENCE {
3122    4:           OCTET STRING 00 00 00 02
        :            }
3128 1290:          [1] {
3132  959:           [0] {
3136  878:            SEQUENCE {
3140    3:             [0] {
3142    1:              INTEGER 2
        :              }
3145   10:             INTEGER 61 4A 76 22 00 00 00 00 00 1D
3157    8:             SEQUENCE {
3159    6:              OBJECT IDENTIFIER
        :               GOST R 34.11/34.10-2001 (1 2 643 2 2 3) (1 2 643 2 2 3)
        :              }
3167  122:             SEQUENCE {
3169   35:              SET {
3171   33:               SEQUENCE {
3173    9:                OBJECT IDENTIFIER
        :                 emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
3184   20:                IA5String 'mivanov@factor-ts.ru'
        :                }
        :               }
3206   11:              SET {
3208    9:               SEQUENCE {
3210    3:                OBJECT IDENTIFIER
        :                 countryName (2 5 4 6) (2 5 4 6)
3215    2:                PrintableString 'RU'
        :                }
        :               }
3219   15:              SET {
3221   13:               SEQUENCE {
3223    3:                OBJECT IDENTIFIER
        :                 localityName (2 5 4 7) (2 5 4 7)
3228    6:                PrintableString 'Moscow'
        :                }
        :               }
```

```
3236   18:              SET {
3238   16:               SEQUENCE {
3240    3:                OBJECT IDENTIFIER
        :                 organizationName (2 5 4 10) (2 5 4 10)
3245    9:                PrintableString 'CryptoPro'
        :                 }
        :                }
3256   14:              SET {
3258   12:               SEQUENCE {
3260    3:                OBJECT IDENTIFIER
        :                 organizationalUnitName (2 5 4 11) (2 5 4 11)
3265    5:                PrintableString 'Promo'
        :                 }
        :                }
3272   17:              SET {
3274   15:               SEQUENCE {
3276    3:                OBJECT IDENTIFIER
        :                 commonName (2 5 4 3) (2 5 4 3)
3281    8:                PrintableString 'Maxim UC'
        :                 }
        :                }
        :               }
3291   30:              SEQUENCE {
3293   13:               UTCTime 18/05/2012 11:03:00 GMT
3308   13:               UTCTime 18/05/2013 11:12:00 GMT
        :                }
3323  186:              SEQUENCE {
3326   35:               SET {
3328   33:                SEQUENCE {
3330    9:                 OBJECT IDENTIFIER
        :                  emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
3341   20:                 IA5String 'fedotov@factor-ts.ru'
        :                 }
        :                }
3363   11:               SET {
3365    9:                SEQUENCE {
3367    3:                 OBJECT IDENTIFIER
        :                  countryName (2 5 4 6) (2 5 4 6)
3372    2:                 PrintableString 'RU'
        :                 }
        :                }
3376   21:               SET {
3378   19:                SEQUENCE {
3380    3:                 OBJECT IDENTIFIER
        :                  localityName (2 5 4 7) (2 5 4 7)
3385   12:                 BMPString '...>.A.:.2.0'
        :                 }
        :                }
3399   27:               SET {
3401   25:                SEQUENCE {
3403    3:                 OBJECT IDENTIFIER
        :                  organizationName (2 5 4 10) (2 5 4 10)
3408   18:                 BMPString '.$.0.:.B.>.@-.".!'
        :                 }
        :                }
3428   17:               SET {
3430   15:                SEQUENCE {
3432    3:                 OBJECT IDENTIFIER
        :                  organizationalUnitName (2 5 4 11) (2 5 4 11)
3437    8:                 BMPString '."5.A.B'
        :                 }
        :                }
3447   63:               SET {
3449   61:                SEQUENCE {
3451    3:                 OBJECT IDENTIFIER
        :                  commonName (2 5 4 3) (2 5 4 3)
3456   54:                 BMPString
        :           '.$.5.4.>.B.>.2 ...=.4.@.5.9 ...;.0.4.8.<.8.@.>.2'
        :           '.8.G'
        :                 }
        :                }
        :               }
3512   99:              SEQUENCE {
3514   28:               SEQUENCE {
3516    6:                OBJECT IDENTIFIER
        :                 GOST R 34.10-2001 (1 2 643 2 2 19) (1 2 643 2 2 19)
3524   18:                SEQUENCE {
3526    7:                 OBJECT IDENTIFIER
```

```
        :                 id-GostR3410-2001-CryptoPro-A-ParamSet (1 2 643 2 2 35 1) (1 2 643 2 2
35 1)
3535    7:                OBJECT IDENTIFIER
        :                 id-GostR3411-94-CryptoProParamSet (1 2 643 2 2 30 1) (1 2 643 2 2 30
1)
        :                 }
        :                }
3544   67:              BIT STRING, encapsulates {
3547   64:               OCTET STRING
        :          ED 92 03 66 00 10 11 B9 AC 32 68 28 56 76 95 D2
        :          4B B1 1F 22 66 82 FC 53 CC 91 CA 6A 0A 14 30 67
        :          27 6A 53 43 D1 E2 93 16 4B 21 00 12 89 47 C8 86
        :          F9 21 44 95 51 08 A7 45 E6 17 85 73 75 9D 64 4E
        :                }
        :               }
3613  401:             [3] {
3617  397:              SEQUENCE {
3621   14:               SEQUENCE {
3623    3:                OBJECT IDENTIFIER
        :                 keyUsage (2 5 29 15) (2 5 29 15)
3628    1:                BOOLEAN TRUE
3631    4:                OCTET STRING, encapsulates {
3633    2:                 BIT STRING 4 unused bits
        :                  '1111'B
        :                 }
        :                }
3637   19:               SEQUENCE {
3639    3:                OBJECT IDENTIFIER
        :                 extKeyUsage (2 5 29 37) (2 5 29 37)
3644   12:                OCTET STRING, encapsulates {
3646   10:                 SEQUENCE {
3648    8:                  OBJECT IDENTIFIER
        :                   iKEIntermediate (1 3 6 1 5 5 8 2 2) (1 3 6 1 5 5 8 2 2)
        :                  }
        :                 }
        :                }
3658   29:               SEQUENCE {
3660    3:                OBJECT IDENTIFIER
        :                 subjectKeyIdentifier (2 5 29 14) (2 5 29 14)
3665   22:                OCTET STRING, encapsulates {
3667   20:                 OCTET STRING
        :          52 58 AD 0C 45 43 0D E5 F6 DE 39 7B 77 3B 3D F9
        :          1D 69 FF 39
        :                 }
        :                }
3689   31:               SEQUENCE {
3691    3:                OBJECT IDENTIFIER
        :                 authorityKeyIdentifier (2 5 29 35) (2 5 29 35)
3696   24:                OCTET STRING, encapsulates {
3698   22:                 SEQUENCE {
3700   20:                  [0]
        :          C3 99 AC 2E F8 F6 FC F0 62 2C 8A 80 35 DF DA 63
        :          28 17 EF ED
        :                  }
        :                 }
        :                }
3722  117:               SEQUENCE {
3724    3:                OBJECT IDENTIFIER
        :                 cRLDistributionPoints (2 5 29 31) (2 5 29 31)
3729  110:                OCTET STRING, encapsulates {
3731  108:                 SEQUENCE {
3733  106:                  SEQUENCE {
3735  104:                   [0] {
3737  102:                    [0] {
3739   48:                     [6]
        :          'http://voenmeh-d0f286a/CertEnroll/Maxim%20UC.crl'
3789   50:                     [6]
        :          'file://\\voenmeh-d0f286a\CertEnroll\Maxim%20UC.c'
        :          'rl'
        :                    }
        :                   }
        :                  }
        :                 }
        :                }
        :               }
3841  174:               SEQUENCE {
3844    8:                OBJECT IDENTIFIER
        :                 authorityInfoAccess (1 3 6 1 5 5 7 1 1) (1 3 6 1 5 5 7 1 1)
3854  161:                OCTET STRING, encapsulates {
```

```
3857  158:                SEQUENCE {
3860   76:                 SEQUENCE {
3862    8:                  OBJECT IDENTIFIER
        :                   caIssuers (1 3 6 1 5 5 7 48 2) (1 3 6 1 5 5 7 48 2)
3872   64:                  [6]
        :           'http://voenmeh-d0f286a/CertEnroll/voenmeh-d0f286'
        :           'a_Maxim%20UC.crt'
        :                  }
3938   78:                 SEQUENCE {
3940    8:                  OBJECT IDENTIFIER
        :                   caIssuers (1 3 6 1 5 5 7 48 2) (1 3 6 1 5 5 7 48 2)
3950   66:                  [6]
        :           'file://\\voenmeh-d0f286a\CertEnroll\voenmeh-d0f2'
        :           '86a_Maxim%20UC.crt'
        :                  }
        :                 }
        :                }
        :               }
        :              }
        :             }
        :            }
4018    8:            SEQUENCE {
4020    6:             OBJECT IDENTIFIER
        :              GOST R 34.11/34.10-2001 (1 2 643 2 2 3) (1 2 643 2 2 3)
        :              }
4028   65:            BIT STRING
        :           71 DB 23 67 25 9C C9 D0 86 2A C9 1D D9 9D AA C8
        :           51 BC A9 2C BA F4 82 F3 F4 8E CF 0C 81 77 A7 2F
        :           35 34 8A D8 9B B1 B0 0A 18 50 A2 7E CF 8A 6D CB
        :           5E 53 21 88 08 EC F3 CA 7A 36 02 8D A2 F1 F5 E4
        :            }
4095  186:           SEQUENCE {
4098   35:            SET {
4100   33:             SEQUENCE {
4102    9:              OBJECT IDENTIFIER
        :               emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
4113   20:              IA5String 'fedotov@factor-ts.ru'
        :              }
        :             }
4135   11:            SET {
4137    9:             SEQUENCE {
4139    3:              OBJECT IDENTIFIER
        :               countryName (2 5 4 6) (2 5 4 6)
4144    2:              PrintableString 'RU'
        :              }
        :             }
4148   21:            SET {
4150   19:             SEQUENCE {
4152    3:              OBJECT IDENTIFIER
        :               localityName (2 5 4 7) (2 5 4 7)
4157   12:              BMPString '...>.A.:.2.0'
        :              }
        :             }
4171   27:            SET {
4173   25:             SEQUENCE {
4175    3:              OBJECT IDENTIFIER
        :               organizationName (2 5 4 10) (2 5 4 10)
4180   18:              BMPString '.$.0.:.B.>.@-.".!'
        :              }
        :             }
4200   17:            SET {
4202   15:             SEQUENCE {
4204    3:              OBJECT IDENTIFIER
        :               organizationalUnitName (2 5 4 11) (2 5 4 11)
4209    8:              BMPString '."5.A.B'
        :              }
        :             }
4219   63:            SET {
4221   61:             SEQUENCE {
4223    3:              OBJECT IDENTIFIER
        :               commonName (2 5 4 3) (2 5 4 3)
4228   54:              BMPString
        :           '.$.5.4.>.B.>.2 ...=.4.@.5.9 ...;.0.4.8.<.8.@.>.2'
        :           '.8.G'
        :              }
        :             }
        :            }
4284  124:           [0] {
4286  122:            SEQUENCE {
```

```
4288   35:             SET {
4290   33:              SEQUENCE {
4292    9:               OBJECT IDENTIFIER
        :                emailAddress (1 2 840 113549 1 9 1) (1 2 840 113549 1 9 1)
4303   20:               IA5String 'mivanov@factor-ts.ru'
        :                }
        :               }
4325   11:             SET {
4327    9:              SEQUENCE {
4329    3:               OBJECT IDENTIFIER
        :                countryName (2 5 4 6) (2 5 4 6)
4334    2:               PrintableString 'RU'
        :                }
        :               }
4338   15:             SET {
4340   13:              SEQUENCE {
4342    3:               OBJECT IDENTIFIER
        :                localityName (2 5 4 7) (2 5 4 7)
4347    6:               PrintableString 'Moscow'
        :                }
        :               }
4355   18:             SET {
4357   16:              SEQUENCE {
4359    3:               OBJECT IDENTIFIER
        :                organizationName (2 5 4 10) (2 5 4 10)
4364    9:               PrintableString 'CryptoPro'
        :                }
        :               }
4375   14:             SET {
4377   12:              SEQUENCE {
4379    3:               OBJECT IDENTIFIER
        :                organizationalUnitName (2 5 4 11) (2 5 4 11)
4384    5:               PrintableString 'Promo'
        :                }
        :               }
4391   17:             SET {
4393   15:              SEQUENCE {
4395    3:               OBJECT IDENTIFIER
        :                commonName (2 5 4 3) (2 5 4 3)
4400    8:               PrintableString 'Maxim UC'
        :                }
        :               }
        :              }
        :             }
4410   10:            INTEGER 61 4A 76 22 00 00 00 00 00 1D
        :            }
        :           }
        :          }
        :         }
4422  320:        [0] {
4426  316:         [0] {
4430  312:          [26] {
4434   31:           SEQUENCE {
4436   25:            UTF8String 'New Generated Private Key'
4463    2:            BIT STRING 7 unused bits
        :             '1'B (bit 0)
        :             }
4467   14:           SEQUENCE {
4469    4:            OCTET STRING 00 00 00 03
4475    2:            BIT STRING 5 unused bits
        :             '001'B (bit 0)
4479    2:            BIT STRING 5 unused bits
        :             '111'B
        :             }
4483  259:           [1] {
4487  245:            [2] {
4490    1:             INTEGER 2
4493   89:             SET {
4495   87:              [2] {
4497    1:               INTEGER 4
4500    6:               SEQUENCE {
4502    4:                OCTET STRING 00 00 00 04
        :                }
4508   30:               SEQUENCE {
4510    7:                OBJECT IDENTIFIER '1 2 643 2 2 13 1'
4519   19:                SEQUENCE {
4521    7:                 OBJECT IDENTIFIER
        :                  id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2
31 1)
```

```
4530    8:               OCTET STRING 26 30 47 72 9C E3 74 6F
        :                }
        :               }
4540   42:              OCTET STRING, encapsulates {
4542   40:               SEQUENCE {
4544   32:                OCTET STRING
        :           D6 B9 95 95 DD 7A D6 C3 E6 7D FC 52 19 6E C6 35
        :           4E 3E 95 0B DE 23 C1 23 CB 76 61 98 E4 2E 75 19
4578    4:                OCTET STRING FD B5 BD 92
        :                }
        :               }
        :              }
        :             }
4584  148:            SEQUENCE {
4587    9:             OBJECT IDENTIFIER
        :              data (1 2 840 113549 1 7 1) (1 2 840 113549 1 7 1)
4598   31:             SEQUENCE {
4600    8:              OBJECT IDENTIFIER '1 2 643 2 4 3 2 2'
4610   19:              SEQUENCE {
4612    8:               OCTET STRING 64 59 E7 C7 14 DE 0A E3
4622    7:               OBJECT IDENTIFIER
        :                id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2 31
1)
        :               }
        :              }
4631  102:             [0]
        :           17 FA 51 6A 7E 0C 59 F3 E8 72 F0 7B 8D BE 3D F1
        :           D6 76 CF D1 18 C9 00 7D B1 90 77 E4 6F 68 10 27
        :           D4 5D 11 A4 8E 75 C1 20 DB 9C 73 A4 8A 93 3C EA
        :           26 9E CF 3E 06 41 E6 02 C4 0B B6 C9 CD 05 06 4E
        :           B5 2B 12 74 09 BE 45 4D E2 98 8C CF 66 FC 5F 57
        :           07 3D B2 41 8B B9 B6 85 FE 0F D4 7F 7B D2 E0 EF
        :           32 2C 62 83 F4 07
        :             }
        :            }
4735    9:           SEQUENCE {
4737    7:            OBJECT IDENTIFIER
        :             id-GostR3410-2001-CryptoPro-B-ParamSet (1 2 643 2 2 35 2) (1 2 643 2 2 35
2)
        :            }
        :           }
        :          }
        :         }
        :        }
4746  146:       [1] {
4749  143:        [0] {
4752  140:         [26] {
4755   45:          SEQUENCE {
4757   40:           UTF8String 'Public Key for New Generated Private Key'
4799    1:           BIT STRING
        :            }
4802   10:          SEQUENCE {
4804    4:           OCTET STRING 00 00 00 03
4810    2:           BIT STRING 1 unused bit
        :            '0000001'B (bit 0)
        :            }
4814   79:          [1] {
4816   66:           [0] {
4818   64:            OCTET STRING
        :           1E 8B CE FD 7C 95 E8 4F 11 E3 5A 14 A0 58 FD 5B
        :           CB 3E 24 89 3A DE 91 59 99 EB 27 5B A3 AF AF 1D
        :           D4 D5 8D 6C 32 A2 64 D3 8A E6 CD 07 54 0C 76 7B
        :           41 5E 64 54 0B E9 23 02 A7 F4 EA FA 65 CD F6 4B
        :             }
4884    9:           SEQUENCE {
4886    7:            OBJECT IDENTIFIER
        :             id-GostR3410-2001-CryptoPro-B-ParamSet (1 2 643 2 2 35 2) (1 2 643 2 2 35
2)
        :            }
        :           }
        :          }
        :         }
        :        }
4895  288:       [7] {
4899  284:        [0] {
4903  280:         [1] {
4907   21:          SEQUENCE {
4909   15:           UTF8String 'Top-secret Data'
4926    2:           BIT STRING 6 unused bits
```

```
         :           '11'B
         :           }
4930   13:         SEQUENCE {
4932   11:          OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 4'
         :           }
4945  239:         [1] {
4948    5:          OBJECT IDENTIFIER '1 1 456 7890'
4955  229:          [2] {
4958    1:           INTEGER 2
4961   89:           SET {
4963   87:            [2] {
4965    1:             INTEGER 4
4968    6:             SEQUENCE {
4970    4:              OCTET STRING 00 00 00 04
         :              }
4976   30:             SEQUENCE {
4978    7:              OBJECT IDENTIFIER '1 2 643 2 2 13 1'
4987   19:              SEQUENCE {
4989    7:               OBJECT IDENTIFIER
         :                id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2
31 1)
4998    8:               OCTET STRING 72 1F F5 35 95 22 EC C2
         :               }
         :              }
5008   42:             OCTET STRING, encapsulates {
5010   40:              SEQUENCE {
5012   32:               OCTET STRING
         :           F2 D2 EE E6 12 44 64 20 97 1F 02 A7 D2 0C C5 D5
         :           77 46 96 F0 3D F8 B5 62 3D A9 45 0A E6 DF 6D 64
5046    4:                OCTET STRING E2 0A 7F 02
         :               }
         :              }
         :             }
         :            }
5052  132:           SEQUENCE {
5055    9:            OBJECT IDENTIFIER
         :             data (1 2 840 113549 1 7 1) (1 2 840 113549 1 7 1)
5066   31:            SEQUENCE {
5068    8:             OBJECT IDENTIFIER '1 2 643 2 4 3 2 2'
5078   19:             SEQUENCE {
5080    8:              OCTET STRING 3F 90 96 7B F8 3F 30 1D
5090    7:              OBJECT IDENTIFIER
         :               id-Gost28147-89-CryptoPro-A-ParamSet (1 2 643 2 2 31 1) (1 2 643 2 2 31
1)
         :              }
         :             }
5099   86:            [0]
         :           15 9D C1 8F 62 07 70 D0 03 31 74 DF A7 02 5C D9
         :           22 3C F2 97 AA D5 D4 F1 C5 E7 06 04 64 F9 73 2E
         :           64 B4 5B C2 50 4A 52 64 B0 A9 FB 07 27 F5 37 58
         :           EF 4D B0 BD A3 69 A1 A8 77 2C 15 25 8E 50 07 8F
         :           E0 CA 14 EF F6 3A C1 16 19 76 C9 31 DB A3 37 6D
         :           96 F6 8C 81 6B 68
         :            }
         :           }
         :          }
         :         }
         :        }
5187  107:       [7] {
5189  105:        [0] {
5191  103:         [1] {
5193   17:          SEQUENCE {
5195   11:           UTF8String 'Public Data'
5208    2:           BIT STRING 6 unused bits
         :            '01'B (bit 0)
         :           }
5212   13:          SEQUENCE {
5214   11:           OBJECT IDENTIFIER '1 3 6 1 4 1 13312 503 1 4'
         :           }
5227   67:          [1] {
5229    6:           OBJECT IDENTIFIER '1 1 765 432 1'
5237   57:           [0] {
5239   55:            OCTET STRING
         :           'This is some open data. There's no need to encry'
         :           'pt it..'
         :             }
         :            }
         :           }
```

```
         :          }
         :         }
         :        }
         :       }
         :      }
         :     }
         :    }
5296   76:  [2] {
5298   25:   SEQUENCE {
5300    9:    OBJECT IDENTIFIER
         :     contentType (1 2 840 113549 1 9 3) (1 2 840 113549 1 9 3)
5311   12:    SET {
5313   10:     OBJECT IDENTIFIER
         :      pkcs15content (1 2 840 113549 1 15 3 1) (1 2 840 113549 1 15 3 1)
         :      }
         :     }
5325   47:   SEQUENCE {
5327    9:    OBJECT IDENTIFIER
         :     messageDigest (1 2 840 113549 1 9 4) (1 2 840 113549 1 9 4)
5338   34:    SET {
5340   32:     OCTET STRING
         :      64 4E D1 DA ED D7 ED BB 0A D8 1C 4E A8 03 4E 41
         :      F9 04 A7 D0 02 15 23 3A 83 9C 7E EE B0 BE 74 68
         :      }
         :     }
         :    }
5374   32:  OCTET STRING
         :   FA FD 4D 0E 63 7F 29 11 59 1D 5D 3F AF A6 0C C4
         :   E7 F1 36 2E 93 59 E2 5C D5 68 E5 B0 FA 5B 15 39
         :   }
```

Процесс формирования Software Token:

```
p15_add_cert:
p15_add_cert: Adding certificate 'Root Certificate of CA':
trusted: 1
ca: 1
certificate (701 bytes):
30 82 02 B9  30 82 02 68  A0 03 02 01  02 02 10 07  |0...0..h........|
48 BA C5 90  EA C5 9B 4C  4F 0F E7 04  98 9C A8 30  |H......LO......0|
08 06 06 2A  85 03 02 02  03 30 7A 31  23 30 21 06  |...*.....0z1#0!.|
09 2A 86 48  86 F7 0D 01  09 01 16 14  6D 69 76 61  |.*.H........miva|
6E 6F 76 40  66 61 63 74  6F 72 2D 74  73 2E 72 75  |nov@factor-ts.ru|
31 0B 30 09  06 03 55 04  06 13 02 52  55 31 0F 30  |1.0...U....RU1.0|
0D 06 03 55  04 07 13 06  4D 6F 73 63  6F 77 31 12  |...U....Moscow1.|
30 10 06 03  55 04 0A 13  09 43 72 79  70 74 6F 50  |0...U....CryptoP|
72 6F 31 0E  30 0C 06 03  55 04 0B 13  05 50 72 6F  |ro1.0...U....Pro|
6D 6F 31 11  30 0F 06 03  55 04 03 13  08 4D 61 78  |mo1.0...U....Max|
69 6D 20 55  43 30 1E 17  0D 31 32 30  33 32 31 31  |im UC0...1203211|
32 33 39 33  38 5A 17 0D  31 37 30 33  32 31 31 32  |23938Z..17032112|
34 36 31 32  5A 30 7A 31  23 30 21 06  09 2A 86 48  |4612Z0z1#0!..*.H|
86 F7 0D 01  09 01 16 14  6D 69 76 61  6E 6F 76 40  |........mivanov@|
66 61 63 74  6F 72 2D 74  73 2E 72 75  31 0B 30 09  |factor-ts.ru1.0.|
06 03 55 04  06 13 02 52  55 31 0F 30  0D 06 03 55  |..U....RU1.0...U|
04 07 13 06  4D 6F 73 63  6F 77 31 12  30 10 06 03  |....Moscow1.0...|
55 04 0A 13  09 43 72 79  70 74 6F 50  72 6F 31 0E  |U....CryptoPro1.|
30 0C 06 03  55 04 0B 13  05 50 72 6F  6D 6F 31 11  |0...U....Promo1.|
30 0F 06 03  55 04 03 13  08 4D 61 78  69 6D 20 55  |0...U....Maxim U|
43 30 63 30  1C 06 06 2A  85 03 02 02  13 30 12 06  |C0c0...*.....0..|
07 2A 85 03  02 02 23 01  06 07 2A 85  03 02 02 1E  |.*....#...*.....|
01 03 43 00  04 40 97 CB  DD 42 DF 80  28 13 B2 99  |..C..@...B..(...|
11 64 6B E1  38 12 02 1F  6E 83 5F B3  35 B1 48 15  |.dk.8...n._.5.H.|
E0 43 CD 76  24 6D 8D 70  52 10 B8 61  47 40 CF E2  |.C.v$m.pR..aG@..|
31 4E 54 51  39 D5 CF 23  BB 24 47 59  27 2F D7 9D  |1NTQ9..#.$GY'/..|
F4 42 A8 C4  DD 9C A3 81  C7 30 81 C4  30 0B 06 03  |.B.......0..0...|
55 1D 0F 04  04 03 02 01  86 30 0F 06  03 55 1D 13  |U........0...U..|
01 01 FF 04  05 30 03 01  01 FF 30 1D  06 03 55 1D  |.....0....0...U.|
0E 04 16 04  14 C3 99 AC  2E F8 F6 FC  F0 62 2C 8A  |.............b,.|
80 35 DF DA  63 28 17 EF  ED 30 73 06  03 55 1D 1F  |.5..c(...0s..U..|
04 6C 30 6A  30 68 A0 66  A0 64 86 30  68 74 74 70  |.l0j0h.f.d.0http|
3A 2F 2F 76  6F 65 6E 6D  65 68 2D 64  30 66 32 38  |://voenmeh-d0f28|
36 61 2F 43  65 72 74 45  6E 72 6F 6C  6C 2F 4D 61  |6a/CertEnroll/Ma|
78 69 6D 25  32 30 55 43  2E 63 72 6C  86 30 66 69  |xim%20UC.crl.0fi|
6C 65 3A 2F  2F 5C 5C 76  6F 65 6E 6D  65 68 2D 64  |le://\\voenmeh-d|
30 66 32 38  36 61 5C 43  65 72 74 45  6E 72 6F 6C  |0f286a\CertEnrol|
6C 5C 4D 61  78 69 6D 20  55 43 2E 63  72 6C 30 10  |l\Maxim UC.crl0.|
```

```
06 09 2B 06  01 04 01 82  37 15 01 04  03 02 01 00  |..+.....7.......|
30 08 06 06  2A 85 03 02  02 03 03 41  00 C1 74 E0  |0...*......A..t.|
FC 28 6F 84  9C BA FA 24  ED A3 AB D1  44 97 D4 E2  |.(o....$....D...|
46 74 C2 D4  9E B9 F8 1B  53 1C 98 BA  AA 95 DB EB  |Ft......S.......|
DA 76 A2 45  2F 05 99 F1  96 B3 9F 2F  F1 71 E5 12  |.v.E/....../.q..|
66 CB EB 59  39 32 F5 7B  6A D0 7C F8  AD           |f..Y92.{j.|..   |

p15_add_crl: Adding CRL 'CRL from CA':
crl (690 bytes):
30 82 02 AE  30 82 02 5D  02 01 01 30  08 06 06 2A  |0...0..]...0...*|
85 03 02 02  03 30 7A 31  23 30 21 06  09 2A 86 48  |.....0z1#0!..*.H|
86 F7 0D 01  09 01 16 14  6D 69 76 61  6E 6F 76 40  |........mivanov@|
66 61 63 74  6F 72 2D 74  73 2E 72 75  31 0B 30 09  |factor-ts.ru1.0.|
06 03 55 04  06 13 02 52  55 31 0F 30  0D 06 03 55  |..U....RU1.0...U|
04 07 13 06  4D 6F 73 63  6F 77 31 12  30 10 06 03  |....Moscow1.0...|
55 04 0A 13  09 43 72 79  70 74 6F 50  72 6F 31 0E  |U....CryptoPro1.|
30 0C 06 03  55 04 0B 13  05 50 72 6F  6D 6F 31 11  |0...U....Promo1.|
30 0F 06 03  55 04 03 13  08 4D 61 78  69 6D 20 55  |0...U....Maxim U|
43 17 0D 31  32 30 35 31  35 30 39 31  30 30 36 5A  |C..120515091006Z|
17 0D 31 32  30 35 32 32  32 31 33 30  30 36 5A 30  |..120522213006Z0|
81 81 30 29  02 0A 61 04  D6 67 00 00  00 00 00 12  |..0)..a..g......|
17 0D 31 32  30 35 30 32  31 31 34 31  32 37 5A 30  |..120502114127Z0|
0C 30 0A 06  03 55 1D 15  04 03 0A 01  05 30 29 02  |.0...U.......0).|
0A 61 10 5F  A6 00 00 00  00 00 07 17  0D 31 32 30  |.a._.........120|
35 30 32 31  31 33 38 32  30 5A 30 0C  30 0A 06 03  |502113820Z0.0...|
55 1D 15 04  03 0A 01 05  30 29 02 0A  61 E9 42 A9  |U.......0)..a.B.|
00 00 00 00  00 11 17 0D  31 32 30 35  30 32 31 31  |........12050211|
33 38 30 35  5A 30 0C 30  0A 06 03 55  1D 15 04 03  |3805Z0.0...U....|
0A 01 05 A0  82 01 2E 30  82 01 2A 30  1F 06 03 55  |.......0..*0...U|
1D 23 04 18  30 16 80 14  C3 99 AC 2E  F8 F6 FC F0  |.#..0...........|
62 2C 8A 80  35 DF DA 63  28 17 EF ED  30 10 06 09  |b,..5..c(...0...|
2B 06 01 04  01 82 37 15  01 04 03 02  01 00 30 0A  |+.....7.......0.|
06 03 55 1D  14 04 03 02  01 05 30 1C  06 09 2B 06  |..U.......0...+.|
01 04 01 82  37 15 04 04  0F 17 0D 31  32 30 35 32  |....7......12052|
32 30 39 32  30 30 36 5A  30 81 CA 06  09 2B 06 01  |2092006Z0....+..|
04 01 82 37  15 0E 04 81  BC 30 81 B9  30 81 B6 A0  |...7.....0..0...|
81 B3 A0 81  B0 86 81 AD  6C 64 61 70  3A 2F 2F 2F  |........ldap:///|
43 4E 3D 4D  61 78 69 6D  25 32 30 55  43 2C 43 4E  |CN=Maxim%20UC,CN|
3D 76 6F 65  6E 6D 65 68  2D 64 30 66  32 38 36 61  |=voenmeh-d0f286a|
2C 43 4E 3D  43 44 50 2C  43 4E 3D 50  75 62 6C 69  |,CN=CDP,CN=Publi|
63 25 32 30  4B 65 79 25  32 30 53 65  72 76 69 63  |c%20Key%20Servic|
65 73 2C 43  4E 3D 53 65  72 76 69 63  65 73 2C 44  |es,CN=Services,D|
43 3D 55 6E  61 76 61 69  6C 61 62 6C  65 43 6F 6E  |C=UnavailableCon|
66 69 67 44  4E 3F 63 65  72 74 69 66  69 63 61 74  |figDN?certificat|
65 52 65 76  6F 63 61 74  69 6F 6E 4C  69 73 74 3F  |eRevocationList?|
62 61 73 65  3F 6F 62 6A  65 63 74 43  6C 61 73 73  |base?objectClass|
3D 63 52 4C  44 69 73 74  72 69 62 75  74 69 6F 6E  |=cRLDistribution|
50 6F 69 6E  74 30 08 06  06 2A 85 03  02 02 03 03  |Point0...*......|
41 00 70 B6  42 8A 9A E3  05 82 9E 7F  5B 97 A1 6A  |A.p.B.......[..j|
B1 84 FB F8  23 E7 F2 CD  02 A3 02 92  E8 53 83 8F  |....#........S..|
51 F4 88 A4  0C 37 C6 9D  3C 4B AB 0C  3A A1 0C 0B  |Q....7..<K..:...|
7F 02 35 02  77 88 D2 A3  04 FD 67 EC  9B 92 B0 83  |..5.w.....g.....|
AB 57                                              |.W              |

p15_add_private_key: Adding key 'Private Key of Andrey Fedotov':
key usage: DECRYPT SIGN UNWRAP NON_REPUDIATION
key access: SENSITIVE EXTRACTABLE ALWAYSSENSITIVE
key parameters (1-5 - cproA,B,C,XchA,XchB): 1
start date: 2012-05-18 11:03:00
end date: 2013-05-18 11:12:00
key (little-endian):
D8 DB F1 EE  28 84 7D 4C  4C 0B D6 09  96 34 1C 23  |....(.}LL....4.#|
DB A6 13 77  C8 68 7C CD  58 53 5E 44  D4 24 E8 B3  |...w.h|.XS^D.$..|

Remasking private key 'Private Key of Andrey Fedotov':
Unmasked key (little-endian):
D8 DB F1 EE  28 84 7D 4C  4C 0B D6 09  96 34 1C 23  |....(.}LL....4.#|
DB A6 13 77  C8 68 7C CD  58 53 5E 44  D4 24 E8 B3  |...w.h|.XS^D.$..|
Masked key (little-endian):
C5 F7 B3 4F  ED A8 10 1D  07 54 A0 07  CD A7 57 9F  |...O.....T....W.|
26 95 D0 B8  54 5D 40 62  C0 B9 EA 51  59 94 19 3B  |&...T]@b...QY..;|
Mask 1:
8D 20 1F 80  E5 92 33 96  41 B7 26 D4  B5 D5 26 4A  |. ....3.A.&...&J|
10 8B 3C A6  64 1F BB 81  FA 72 96 F5  84 A8 3D B6  |..<.d....r....=.|
Mask 2:
4B 4A FA 0E  9A 4A 0A 83  B4 4F 2E BD  05 F4 1B C0  |KJ...J...O......|
70 33 53 F5  CB 5D 5E B1  18 19 3B A4  88 0B 81 3D  |p3S..]^...;....=|

p15_add_cert: Adding certificate 'Certificate of Andrey Fedotov':
```

```
trusted: 0
ca: 0
certificate (963 bytes):
30 82 03 BF  30 82 03 6E  A0 03 02 01  02 02 0A 61  |0...0..n.......a|
4A 76 22 00  00 00 00 00  1D 30 08 06  06 2A 85 03  |Jv".......0...*..|
02 02 03 30  7A 31 23 30  21 06 09 2A  86 48 86 F7  |...0z1#0!..*.H..|
0D 01 09 01  16 14 6D 69  76 61 6E 6F  76 40 66 61  |......mivanov@fa|
63 74 6F 72  2D 74 73 2E  72 75 31 0B  30 09 06 03  |ctor-ts.ru1.0...|
55 04 06 13  02 52 55 31  0F 30 0D 06  03 55 04 07  |U....RU1.0...U..|
13 06 4D 6F  73 63 6F 77  31 12 30 10  06 03 55 04  |..Moscow1.0...U.|
0A 13 09 43  72 79 70 74  6F 50 72 6F  31 0E 30 0C  |...CryptoPro1.0.|
06 03 55 04  0B 13 05 50  72 6F 6D 6F  31 11 30 0F  |..U....Promo1.0.|
06 03 55 04  03 13 08 4D  61 78 69 6D  20 55 43 30  |..U....Maxim UC0|
1E 17 0D 31  32 30 35 31  38 31 31 30  33 30 30 5A  |...120518110300Z|
17 0D 31 33  30 35 31 38  31 31 31 32  30 30 5A 30  |..130518111200Z0|
81 BA 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |..1#0!..*.H.....|
01 16 14 66  65 64 6F 74  6F 76 40 66  61 63 74 6F  |...fedotov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 15 30 13  06 03 55 04  07 1E 0C 04  |..RU1.0...U.....|
1C 04 3E 04  41 04 3A 04  32 04 30 31  1B 30 19 06  |..>.A.:.2.01.0..|
03 55 04 0A  1E 12 04 24  04 30 04 3A  04 42 04 3E  |.U.....$.0.:.B.>|
04 40 00 2D  04 22 04 21  31 11 30 0F  06 03 55 04  |.@.-."."!1.0...U.|
0B 1E 08 04  22 04 35 04  41 04 42 31  3F 30 3D 06  |...."."5.A.B1?0=.|
03 55 04 03  1E 36 04 24  04 35 04 34  04 3E 04 42  |.U...6.$.5.4.>.B|
04 3E 04 32  00 20 04 10  04 3D 04 34  04 40 04 35  |.>.2. ...=.4.@.5|
04 39 00 20  04 12 04 3B  04 30 04 34  04 38 04 3C  |.9. ...;.0.4.8.<|
04 38 04 40  04 3E 04 32  04 38 04 47  30 63 30 1C  |.8.@.>.2.8.G0c0.|
06 06 2A 85  03 02 02 13  30 12 06 07  2A 85 03 02  |..*.....0...*...|
02 23 01 06  07 2A 85 03  02 02 1E 01  03 43 00 04  |.#...*.......C..|
40 ED 92 03  66 00 10 11  B9 AC 32 68  28 56 76 95  |@...f.....2h(Vv.|
D2 4B B1 1F  22 66 82 FC  53 CC 91 CA  6A 0A 14 30  |.K.."f..S...j..0|
67 27 6A 53  43 D1 E2 93  16 4B 21 00  12 89 47 C8  |g'jSC....K!...G.|
86 F9 21 44  95 51 08 A7  45 E6 17 85  73 75 9D 64  |..!D.Q..E...su.d|
4E A3 82 01  91 30 82 01  8D 30 0E 06  03 55 1D 0F  |N....0...0...U..|
01 01 FF 04  04 03 02 04  F0 30 13 06  03 55 1D 25  |.........0...U.%|
04 0C 30 0A  06 08 2B 06  01 05 05 08  02 02 30 1D  |..0...+.......0.|
06 03 55 1D  0E 04 16 04  14 52 58 AD  0C 45 43 0D  |..U......RX..EC.|
E5 F6 DE 39  7B 77 3B 3D  F9 1D 69 FF  39 30 1F 06  |...9{w;=..i.90..|
03 55 1D 23  04 18 30 16  80 14 C3 99  AC 2E F8 F6  |.U.#..0.........|
FC F0 62 2C  8A 80 35 DF  DA 63 28 17  EF ED 30 75  |..b,..5..c(...0u|
06 03 55 1D  1F 04 6E 30  6C 30 6A A0  68 A0 66 86  |..U...n0l0j.h.f.|
30 68 74 74  70 3A 2F 2F  76 6F 65 6E  6D 65 68 2D  |0http://voenmeh-|
64 30 66 32  38 36 61 2F  43 65 72 74  45 6E 72 6F  |d0f286a/CertEnro|
6C 6C 2F 4D  61 78 69 6D  25 32 30 55  43 2E 63 72  |ll/Maxim%20UC.cr|
6C 86 32 66  69 6C 65 3A  2F 2F 5C 5C  76 6F 65 6E  |l.2file://\\voen|
6D 65 68 2D  64 30 66 32  38 36 61 5C  43 65 72 74  |meh-d0f286a\Cert|
45 6E 72 6F  6C 6C 5C 4D  61 78 69 6D  25 32 30 55  |Enroll\Maxim%20U|
43 2E 63 72  6C 30 81 AE  06 08 2B 06  01 05 05 07  |C.crl0....+.....|
01 01 04 81  A1 30 81 9E  30 4C 06 08  2B 06 01 05  |.....0..0L..+...|
05 07 30 02  86 40 68 74  74 70 3A 2F  2F 76 6F 65  |..0..@http://voe|
6E 6D 65 68  2D 64 30 66  32 38 36 61  2F 43 65 72  |nmeh-d0f286a/Cer|
74 45 6E 72  6F 6C 6C 2F  76 6F 65 6E  6D 65 68 2D  |tEnroll/voenmeh-|
64 30 66 32  38 36 61 5F  4D 61 78 69  6D 25 32 30  |d0f286a_Maxim%20|
55 43 2E 63  72 74 30 4E  06 08 2B 06  01 05 05 07  |UC.crt0N..+.....|
30 02 86 42  66 69 6C 65  3A 2F 2F 5C  5C 76 6F 65  |0..Bfile://\\voe|
6E 6D 65 68  2D 64 30 66  32 38 36 61  5C 43 65 72  |nmeh-d0f286a\Cer|
74 45 6E 72  6F 6C 6C 5C  76 6F 65 6E  6D 65 68 2D  |tEnroll\voenmeh-|
64 30 66 32  38 36 61 5F  4D 61 78 69  6D 25 32 30  |d0f286a_Maxim%20|
55 43 2E 63  72 74 30 08  06 06 2A 85  03 02 02 03  |UC.crt0...*.....|
03 41 00 71  DB 23 67 25  9C C9 D0 86  2A C9 1D D9  |.A.q.#g%....*...|
9D AA C8 51  BC A9 2C BA  F4 82 F3 F4  8E CF 0C 81  |...Q..,.........|
77 A7 2F 35  34 8A D8 9B  B1 B0 0A 18  50 A2 7E CF  |w./54.......P.~.|
8A 6D CB 5E  53 21 88 08  EC F3 CA 7A  36 02 8D A2  |.m.^S!.....z6...|
F1 F5 E4                                          |...             |

p15_add_private_key: Adding key 'New Generated Private Key':
key usage: SIGN
key access: SENSITIVE EXTRACTABLE ALWAYSSENSITIVE
key parameters (1-5 - cproA,B,C,XchA,XchB): 2
start date: absent
end date: absent
key (little-endian):
71 C6 2A 26  C9 CC 94 BE  89 BE 5F 12  18 F0 B2 AB  |q.*&......_.....|
BF 20 50 C1  68 70 70 3B  6F EC 56 A7  9B F0 FA 72  |. P.hpp;o.V....r|

Remasking private key 'New Generated Private Key':
Unmasked key (little-endian):
71 C6 2A 26  C9 CC 94 BE  89 BE 5F 12  18 F0 B2 AB  |q.*&......_.....|
BF 20 50 C1  68 70 70 3B  6F EC 56 A7  9B F0 FA 72  |. P.hpp;o.V....r|
```

```
Masked key (little-endian):
09 31 E6 3C  BD 14 0A F3  29 65 47 A6  93 2A 01 AC  |.1.<....)eG..*..|
32 7B B3 01  6D ED 53 77  CB 1C 3B 5F  02 FD CE 12  |2{..m.Sw..;_....|
Mask 1:
B7 6D E5 26  5C 83 3F 86  AC BD BE D5  AE C1 F1 92  |.m.&\.?.........|
DD 63 D8 78  B8 0D 6A D9  97 2D 4B 2C  20 E7 72 2E  |.c.x..j..-K, .r.|
Mask 2:
ED 67 60 4F  56 32 EF 45  7F 4F 91 80  45 4A DF 7F  |.g`OV2.E.O..EJ..|
FB 4C B9 16  21 7C F2 EF  BB 1A 73 09  78 B0 9B BA  |.L..!|....s.x...|

p15_add_public_key: Adding key 'Public Key for New Generated Private Key'
key usage: VERIFY
key parameters (1-5 - cproA,B,C,XchA,XchB): 2
start date: absent
end date: absent
key (little-endian):
1E 8B CE FD  7C 95 E8 4F  11 E3 5A 14  A0 58 FD 5B  |....|..O..Z..X.[|
CB 3E 24 89  3A DE 91 59  99 EB 27 5B  A3 AF AF 1D  |.>$.:..Y..'[....|
D4 D5 8D 6C  32 A2 64 D3  8A E6 CD 07  54 0C 76 7B  |...l2.d.....T.v{|
41 5E 64 54  0B E9 23 02  A7 F4 EA FA  65 CD F6 4B  |A^dT..#.....e..K|

p15_add_oiddo: Adding abstract data object 'Top-secret Data':
oid: 1.1.456.7890
to_encrypt: 1
data (80 bytes):
54 68 69 73  20 69 73 20  73 6F 6D 65  20 63 6F 6E  |This is some con|
66 69 64 65  6E 74 69 61  6C 20 61 62  73 74 72 61  |fidential abstra|
63 74 20 64  61 74 61 2E  20 49 74 20  77 69 6C 6C  |ct data. It will|
20 62 65 20  65 6E 63 72  79 70 74 65  64 20 69 6E  | be encrypted in|
20 74 68 65  20 63 6F 6E  74 61 69 6E  65 72 2E 00  | the container..|

p15_add_oiddo: Adding abstract data object 'Public Data':
oid: 1.1.765.432.1
to_encrypt: 0
data (55 bytes):
54 68 69 73  20 69 73 20  73 6F 6D 65  20 6F 70 65  |This is some ope|
6E 20 64 61  74 61 2E 20  54 68 65 72  65 27 73 20  |n data. There's |
6E 6F 20 6E  65 65 64 20  74 6F 20 65  6E 63 72 79  |no need to encry|
70 74 20 69  74 2E 00                               |pt it..          |

p15_get_pwkey: Generating the password key from the password using PBKDF2.
Input password:
31 32 33                                            |123              |
Iteration count: 2000
Salt:
F4 53 80 45  B0 2F C8 C6  DE AA 01 ED  A5 16 21 DD  |.S.E./........!.|
B1 65 FB 1F  53 AB C9 4C  1D 64 B3 BD  3F D9 D8 0C  |.e..S..L.d..?...|
Generated password key:
23 75 43 93  A8 7F 82 88  38 EE 0F D9  17 2D 8C AC  |#uC.....8....-..|
57 E0 66 4F  95 3B 3C 3F  70 EA 72 93  00 0A 8D 88  |W.fO.;<?p.r.....|

Making KEKRecipientInfo for AuthenticatedData:
kekri.kekid.keyIdentifier:
00 00 00 04                                         |....             |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
74 BA EE A0  BE CB 77 5E                            |t.....w^         |
Key wrap:
Pw key:
23 75 43 93  A8 7F 82 88  38 EE 0F D9  17 2D 8C AC  |#uC.....8....-..|
57 E0 66 4F  95 3B 3C 3F  70 EA 72 93  00 0A 8D 88  |W.fO.;<?p.r.....|
Session key:
D9 89 7F 8D  E7 98 F6 9A  45 85 8B 89  76 62 50 7C  |........E...vbP||
C5 63 3F A4  F5 0C F5 A0  49 68 9B 63  1F F3 61 09  |.c?.....Ih.c..a.|
Wrapped key:
5E B1 D1 B6  42 1A 02 DE  0B C6 FC 8C  3E 8D 81 0D  |^...B.......>...|
DF 8D 44 08  5D 54 EF 7E  A2 77 6E 19  DA 3E 78 A1  |..D.]T.~.wn..>x.|
MAC of key:
39 93 A8 0D                                         |9...             |
kekri.encryptedKey content:
30 28 04 20  5E B1 D1 B6  42 1A 02 DE  0B C6 FC 8C  |0(. ^...B.......|
3E 8D 81 0D  DF 8D 44 08  5D 54 EF 7E  A2 77 6E 19  |>.....D.]T.~.wn.|
DA 3E 78 A1  04 04 39 93  A8 0D                     |.>x...9...       |

AuthenticatedData.macAlgorithm.algorithm: 1.2.643.2.2.10
AuthenticatedData.digestAlgorithm.algorithm: 1.2.643.2.2.9
AuthenticatedData.encapContentInfo.eContentType: 1.2.840.113549.1.15.3.1
```

```
Making PKCS15Token:

token.keyManagementInfo.keyId:
00 00 00 04                                       |....            |
token.keyManagementInfo.keyInfo.passwordInfo.algId.algorithm: 1.2.840.113549.1.5.12
Making token.keyManagementInfo.keyInfo.passwordInfo.algId.parameters (PBKDF2-params):
par.salt.specified:
F4 53 80 45  B0 2F C8 C6  DE AA 01 ED  A5 16 21 DD  |.S.E./........!.|
B1 65 FB 1F  53 AB C9 4C  1D 64 B3 BD  3F D9 D8 0C  |.e..S..L.d..?...|
par.iterationCount:
07 D0                                             |..              |
par.keyLength: 32
par.prf.algorithm: 1.2.643.2.2.10
token.keyManagementInfo.keyInfo.passwordInfo.algId.parameters (encoded):
30 33 04 20  F4 53 80 45  B0 2F C8 C6  DE AA 01 ED  |03. .S.E./......|
A5 16 21 DD  B1 65 FB 1F  53 AB C9 4C  1D 64 B3 BD  |..!..e..S..L.d..|
3F D9 D8 0C  02 02 07 D0  02 01 20 30  08 06 06 2A  |?......... 0...*|
85 03 02 02  0A                                   |.....           |

Making token.pkcs15Objects:

Making Factor-TS version DataObject:
Setting DataType.oidDO choice.
oidDO.commonObjectAttributes.label:
46 61 63 74  6F 72 2D 54  53 20 76 65  72 73 69 6F  |Factor-TS versio|
6E                                                |n               |
oidDO.commonObjectAttributes.flags: 0x00, size=1, unused_bits=6
oidDO.classAttributes.applicationOID: 1.3.6.1.4.1.13312.503.1.3
oidDO.typeAttributes.id: 1.3.6.1.4.1.13312.503.1.3
Choosing oidDO.typeAttributes.value.direct choice.
FactorTSVersion.majorVersion: 2
FactorTSVersion.minorVersion: 0
Encoded oidDO.typeAttributes.value.direct:
30 06 02 01  02 80 01 00                          |0.......        |

Making RandomInitValue DataObject:
Choosing DataType.oidDO choice.
oidDO.commonObjectAttributes.label:
52 61 6E 64  6F 6D 20 49  6E 69 74 20  56 61 6C 75  |Random Init Valu|
65                                                |e               |
oidDO.commonObjectAttributes.flags: 0xC0, len=1, unused_bits=6
oidDO.classAttributes.applicationOID: 1.3.6.1.4.1.13312.503.1.1
oidDO.typeAttributes.id: 1.3.6.1.4.1.13312.503.1.1
Choosing oidDO.typeAttributes.value.direct-protected.
Making RandomInitValue:
RandomInitValue.randomInit:
4E C9 BA B5  2E 01 4A A0  EE DF F0 96  80 14 53 6A  |N.....J.......Sj|
8E F4 1B CB  76 F4 D3 E3  98 A6 AB 68  37 97 9C A8  |....v......h7...|
8C 80 B6 55  B5 A7 F2 9F  29 29 8C 49  6D 80 04 E6  |...U....)).Im...|
6F F7 A3 E4  A0 AA E2 F7  DD F1 A2 27  C9 6B C9 00  |o..........'.k..|
RandomInitValue.moreRandom:
4F E7 0B 85  60 9C A1 78  F5 FE 73 B6  B2 AC 0D     |O...`..x..s.... |
Encoded RandomInitValue:
30 53 04 40  4E C9 BA B5  2E 01 4A A0  EE DF F0 96  |0S.@N.....J.....|
80 14 53 6A  8E F4 1B CB  76 F4 D3 E3  98 A6 AB 68  |..Sj....v......h|
37 97 9C A8  8C 80 B6 55  B5 A7 F2 9F  29 29 8C 49  |7......U....)).I|
6D 80 04 E6  6F F7 A3 E4  A0 AA E2 F7  DD F1 A2 27  |m...o..........'|
C9 6B C9 00  04 0F 4F E7  0B 85 60 9C  A1 78 F5 FE  |.k....O...`..x..|
73 B6 B2 AC  0D                                   |s....           |
Making EnvelopedData of RandomInitValue:
p15_mk_enveloped_data: Making EnvelopedData.recipientInfos (1 kekri):
kekri.kekid.keyIdentifier:
00 00 00 04                                       |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
74 70 70 52  12 2A 80 50                          |tppR.*.P        |
Key wrap:
Pw key:
23 75 43 93  A8 7F 82 88  38 EE 0F D9  17 2D 8C AC  |#uC.....8....-..|
57 E0 66 4F  95 3B 3C 3F  70 EA 72 93  00 0A 8D 88  |W.fO.;<?p.r.....|
Session key:
09 31 3B 2A  61 B3 46 F5  DE D8 52 5D  1A C9 F2 31  |.1;*a.F...R]...1|
3B 7E DE 09  37 66 29 FE  09 35 83 1E  2F 8B 4D 63  |;~..7f)..5../.Mc|
Wrapped key:
5D 7F 85 0F  18 0A 20 A5  FA 27 BC D4  13 77 39 AF  |].....  ..'...w9.|
A3 51 DB E7  3C B3 88 80  BB BE B8 41  5B 42 46 28  |.Q..<......A[BF(|
MAC of key:
5A 69 79 CD                                       |Ziy.            |
```

```
kekri.encryptedKey content:
30 28 04 20  5D 7F 85 0F  18 0A 20 A5  FA 27 BC D4  |0(. ]..... ..'..|
13 77 39 AF  A3 51 DB E7  3C B3 88 80  BB BE B8 41  |.w9..Q..<......A|
5B 42 46 28  04 04 5A 69  79 CD                    |[BF(..Ziy.      |

EnvelopedData.encryptedContentInfo.contentType: 1.2.840.113549.1.7.1
EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.algorithm: 1.2.643.2.4.3.2.2
Making EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.parameters
(Gost28147_89_Parameters):
par.iv
DD 8E C8 00  0F CA 11 88                           |........        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  DD 8E C8 00  0F CA 11 88  06 07 2A 85  |0.............*.|
03 02 02 1F  01                                    |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
93 9B 98 38  70 4A 73 DD  A0 AE AF 87  4C 4A 00 AD  |...8pJs.....LJ..|
62 B8 21 AA  5C 89 C2 FF  92 1C 5C 43  40 54 BC B6  |b.!.\.....\C@T..|
AA 28 D3 14  8B E9 6F 62  F2 06 37 69  25 2C 5D 09  |.(....ob..7i%,].|
C9 26 44 14  23 51 85 DD  99 06 95 02  8E 0B 98 BE  |.&D.#Q..........|
F5 46 55 CF  63 D8 E5 48  7D 63 25 75  2B F4 B1 93  |.FU.c..H}c%u+...|
E6 3E 22 AA  DB DC 46 03  91                       |.>"...F..       |


Adding token.pkcs15Objects.trustedCertificates element:

Making object for certificate 'Root Certificate of CA':
Choosing CertificateType.x509Certificate choice.
x509.commonObjectAttributes.label:
52 6F 6F 74  20 43 65 72  74 69 66 69  63 61 74 65  |Root Certificate|
20 6F 66 20  43 41                                 | of CA          |
x509.commonObjectAttributes.flags: 0x00, len=1, unused_bits=6
x509.classAttributes.iD:
00 00 00 01                                        |....            |
x509.classAttributes.authority: true
Choosing x509.typeAttributes.value.direct choice.
Certificate (701 bytes):
30 82 02 B9  30 82 02 68  A0 03 02 01  02 02 10 07  |0...0..h........|
48 BA C5 90  EA C5 9B 4C  4F 0F E7 04  98 9C A8 30  |H......LO......0|
08 06 06 2A  85 03 02 02  03 30 7A 31  23 30 21 06  |...*.....0z1#0!.|
09 2A 86 48  86 F7 0D 01  09 01 16 14  6D 69 76 61  |.*.H........miva|
6E 6F 76 40  66 61 63 74  6F 72 2D 74  73 2E 72 75  |nov@factor-ts.ru|
31 0B 30 09  06 03 55 04  06 13 02 52  55 31 0F 30  |1.0...U....RU1.0|
0D 06 03 55  04 07 13 06  4D 6F 73 63  6F 77 31 12  |...U....Moscow1.|
30 10 06 03  55 04 0A 13  09 43 72 79  70 74 6F 50  |0...U....CryptoP|
72 6F 31 0E  30 0C 06 03  55 04 0B 13  05 50 72 6F  |ro1.0...U....Pro|
6D 6F 31 11  30 0F 06 03  55 04 03 13  08 4D 61 78  |mo1.0...U....Max|
69 6D 20 55  43 30 1E 17  0D 31 32 30  33 32 31 31  |im UC0...1203211|
32 33 39 33  38 5A 17 0D  31 37 30 33  32 31 31 32  |23938Z..17032112|
34 36 31 32  5A 30 7A 31  23 30 21 06  09 2A 86 48  |4612Z0z1#0!..*.H|
86 F7 0D 01  09 01 16 14  6D 69 76 61  6E 6F 76 40  |........mivanov@|
66 61 63 74  6F 72 2D 74  73 2E 72 75  31 0B 30 09  |factor-ts.ru1.0.|
06 03 55 04  06 13 02 52  55 31 0F 30  0D 06 03 55  |..U....RU1.0...U|
04 07 13 06  4D 6F 73 63  6F 77 31 12  30 10 06 03  |....Moscow1.0...|
55 04 0A 13  09 43 72 79  70 74 6F 50  72 6F 31 0E  |U....CryptoPro1.|
30 0C 06 03  55 04 0B 13  05 50 72 6F  6D 6F 31 11  |0...U....Promo1.|
30 0F 06 03  55 04 03 13  08 4D 61 78  69 6D 20 55  |0...U....Maxim U|
43 30 63 30  1C 06 06 2A  85 03 02 02  13 30 12 06  |C0c0...*.....0..|
07 2A 85 03  02 02 23 01  06 07 2A 85  03 02 02 1E  |.*....#...*.....|
01 03 43 00  04 40 97 CB  DD 42 DF 80  28 13 B2 99  |..C..@...B..(...|
11 64 6B E1  38 12 02 1F  6E 83 5F B3  35 B1 48 15  |.dk.8...n._.5.H.|
E0 43 CD 76  24 6D 8D 70  52 10 B8 61  47 40 CF E2  |.C.v$m.pR..aG@..|
31 4E 54 51  39 D5 CF 23  BB 24 47 59  27 2F D7 9D  |1NTQ9..#.$GY'/..|
F4 42 A8 C4  DD 9C A3 81  C7 30 81 C4  30 0B 06 03  |.B.......0..0...|
55 1D 0F 04  04 03 02 01  86 30 0F 06  03 55 1D 13  |U........0...U..|
01 01 FF 04  05 30 03 01  01 FF 30 1D  06 03 55 1D  |.....0....0...U.|
0E 04 16 04  14 C3 99 AC  2E F8 F6 FC  F0 62 2C 8A  |.............b,.|
80 35 DF DA  63 28 17 EF  ED 30 73 06  03 55 1D 1F  |.5..c(...0s..U..|
04 6C 30 6A  30 68 A0 66  A0 64 86 30  68 74 74 70  |.l0j0h.f.d.0http|
3A 2F 2F 76  6F 65 6E 6D  65 68 2D 64  30 66 32 38  |://voenmeh-d0f28|
36 61 2F 43  65 72 74 45  6E 72 6F 6C  6C 2F 4D 61  |6a/CertEnroll/Ma|
78 69 6D 25  32 30 55 43  2E 63 72 6C  86 30 66 69  |xim%20UC.crl.0fi|
6C 65 3A 2F  2F 5C 5C 76  6F 65 6E 6D  65 68 2D 64  |le://\\voenmeh-d|
30 66 32 38  36 61 5C 43  65 72 74 45  6E 72 6F 6C  |0f286a\CertEnrol|
6C 5C 4D 61  78 69 6D 20  55 43 2E 63  72 6C 30 10  |l\Maxim UC.crl0.|
06 09 2B 06  01 04 01 82  37 15 01 04  03 02 01 00  |..+.....7.......|
30 08 06 06  2A 85 03 02  02 03 03 41  00 C1 74 E0  |0...*......A..t.|
FC 28 6F 84  9C BA FA 24  ED A3 AB D1  44 97 D4 E2  |.(o....$....D...|
```

```
46 74 C2 D4  9E B9 F8 1B  53 1C 98 BA  AA 95 DB EB  |Ft......S.......|
DA 76 A2 45  2F 05 99 F1  96 B3 9F 2F  F1 71 E5 12  |.v.E/....../.q..|
66 CB EB 59  39 32 F5 7B  6A D0 7C F8  AD           |f..Y92.{j.|..   |
x509.typeAttributes.subject:
30 7A 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |0z1#0!..*.H.....|
01 16 14 6D  69 76 61 6E  6F 76 40 66  61 63 74 6F  |...mivanov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 0F 30 0D  06 03 55 04  07 13 06 4D  |..RU1.0...U....M|
6F 73 63 6F  77 31 12 30  10 06 03 55  04 0A 13 09  |oscow1.0...U....|
43 72 79 70  74 6F 50 72  6F 31 0E 30  0C 06 03 55  |CryptoPro1.0...U|
04 0B 13 05  50 72 6F 6D  6F 31 11 30  0F 06 03 55  |....Promo1.0...U|
04 03 13 08  4D 61 78 69  6D 20 55 43               |....Maxim UC    |
x509.typeAttributes.issuer:
30 7A 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |0z1#0!..*.H.....|
01 16 14 6D  69 76 61 6E  6F 76 40 66  61 63 74 6F  |...mivanov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 0F 30 0D  06 03 55 04  07 13 06 4D  |..RU1.0...U....M|
6F 73 63 6F  77 31 12 30  10 06 03 55  04 0A 13 09  |oscow1.0...U....|
43 72 79 70  74 6F 50 72  6F 31 0E 30  0C 06 03 55  |CryptoPro1.0...U|
04 0B 13 05  50 72 6F 6D  6F 31 11 30  0F 06 03 55  |....Promo1.0...U|
04 03 13 08  4D 61 78 69  6D 20 55 43               |....Maxim UC    |


Adding token.pkcs15Objects.dataObjects (CRL) element:

Making CRL object 'CRL from CA'
Choosing DataType.oidDO choice.
oidDO.commonObjectAttributes.label:
43 52 4C 20  66 72 6F 6D  20 43 41                  |CRL from CA     |
oidDO.commonObjectAttributes.flags: 0x00, len=1, unused_bits=6
oidDO.classAttributes.applicationOID: 1.3.6.1.4.1.13312.503.1.2
oidDO.typeAttributes.id: 1.3.6.1.4.1.13312.503.1.2
Choosing oidDO.typeAttributes.value.direct choice.
Making CRLContainer structure:
CRLContainer.iD:
00 00 00 01                                         |....            |
CRLContainer.issuer:
30 7A 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |0z1#0!..*.H.....|
01 16 14 6D  69 76 61 6E  6F 76 40 66  61 63 74 6F  |...mivanov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 0F 30 0D  06 03 55 04  07 13 06 4D  |..RU1.0...U....M|
6F 73 63 6F  77 31 12 30  10 06 03 55  04 0A 13 09  |oscow1.0...U....|
43 72 79 70  74 6F 50 72  6F 31 0E 30  0C 06 03 55  |CryptoPro1.0...U|
04 0B 13 05  50 72 6F 6D  6F 31 11 30  0F 06 03 55  |....Promo1.0...U|
04 03 13 08  4D 61 78 69  6D 20 55 43               |....Maxim UC    |
CRLContainer.crl (690 bytes):
30 82 02 AE  30 82 02 5D  02 01 01 30  08 06 06 2A  |0...0..]...0...*|
85 03 02 02  03 30 7A 31  23 30 21 06  09 2A 86 48  |.....0z1#0!..*.H|
86 F7 0D 01  09 01 16 14  6D 69 76 61  6E 6F 76 40  |........mivanov@|
66 61 63 74  6F 72 2D 74  73 2E 72 75  31 0B 30 09  |factor-ts.ru1.0.|
06 03 55 04  06 13 02 52  55 31 0F 30  0D 06 03 55  |..U....RU1.0...U|
04 07 13 06  4D 6F 73 63  6F 77 31 12  30 10 06 03  |....Moscow1.0...|
55 04 0A 13  09 43 72 79  70 74 6F 50  72 6F 31 0E  |U....CryptoPro1.|
30 0C 06 03  55 04 0B 13  05 50 72 6F  6D 6F 31 11  |0...U....Promo1.|
30 0F 06 03  55 04 03 13  08 4D 61 78  69 6D 20 55  |0...U....Maxim U|
43 17 0D 31  32 30 35 31  35 30 39 31  30 30 36 5A  |C..120515091006Z|
17 0D 31 32  30 35 32 32  32 31 33 30  30 36 5A 30  |..120522213006Z0|
81 81 30 29  02 0A 61 04  D6 67 00 00  00 00 00 12  |..0)..a..g......|
17 0D 31 32  30 35 30 32  31 31 34 31  32 37 5A 30  |..120502114127Z0|
0C 30 0A 06  03 55 1D 15  04 03 0A 01  05 30 29 02  |.0...U.......0).|
0A 61 10 5F  A6 00 00 00  00 00 07 17  0D 31 32 30  |.a._.........120|
35 30 32 31  31 33 38 32  30 5A 30 0C  30 0A 06 03  |502113820Z0.0...|
55 1D 15 04  03 0A 01 05  30 29 02 0A  61 E9 42 A9  |U.......0)..a.B.|
00 00 00 00  00 11 17 0D  31 32 30 35  30 32 31 31  |........12050211|
33 38 30 35  5A 30 0C 30  0A 06 03 55  1D 15 04 03  |3805Z0.0...U....|
0A 01 05 A0  82 01 2E 30  82 01 2A 30  1F 06 03 55  |.......0..*0...U|
1D 23 04 18  30 16 80 14  C3 99 AC 2E  F8 F6 FC F0  |.#..0...........|
62 2C 8A 80  35 DF DA 63  28 17 EF ED  30 10 06 09  |b,..5..c(...0...|
2B 06 01 04  01 82 37 15  01 04 03 02  01 00 30 0A  |+.....7.......0.|
06 03 55 1D  14 04 03 02  01 05 30 1C  06 09 2B 06  |..U.......0...+.|
01 04 01 82  37 15 04 04  0F 17 0D 31  32 30 35 32  |....7......12052|
32 30 39 32  30 30 36 5A  30 81 CA 06  09 2B 06 01  |2092006Z0....+..|
04 01 82 37  15 0E 04 81  BC 30 81 B9  30 81 B6 A0  |...7.....0..0...|
81 B3 A0 81  B0 86 81 AD  6C 64 61 70  3A 2F 2F 2F  |........ldap:///|
43 4E 3D 4D  61 78 69 6D  25 32 30 55  43 2C 43 4E  |CN=Maxim%20UC,CN|
3D 76 6F 65  6E 6D 65 68  2D 64 30 66  32 38 36 61  |=voenmeh-d0f286a|
2C 43 4E 3D  43 44 50 2C  43 4E 3D 50  75 62 6C 69  |,CN=CDP,CN=Publi|
63 25 32 30  4B 65 79 25  32 30 53 65  72 76 69 63  |c%20Key%20Servic|
65 73 2C 43  4E 3D 53 65  72 76 69 63  65 73 2C 44  |es,CN=Services,D|
```

```
43 3D 55 6E  61 76 61 69  6C 61 62 6C  65 43 6F 6E  |C=UnavailableCon|
66 69 67 44  4E 3F 63 65  72 74 69 66  69 63 61 74  |figDN?certificat|
65 52 65 76  6F 63 61 74  69 6F 6E 4C  69 73 74 3F  |eRevocationList?|
62 61 73 65  3F 6F 62 6A  65 63 74 43  6C 61 73 73  |base?objectClass|
3D 63 52 4C  44 69 73 74  72 69 62 75  74 69 6F 6E  |=cRLDistribution|
50 6F 69 6E  74 30 08 06  06 2A 85 03  02 02 03 03  |Point0...*......|
41 00 70 B6  42 8A 9A E3  05 82 9E 7F  5B 97 A1 6A  |A.p.B.......[..j|
B1 84 FB F8  23 E7 F2 CD  02 A3 02 92  E8 53 83 8F  |....#........S..|
51 F4 88 A4  0C 37 C6 9D  3C 4B AB 0C  3A A1 0C 0B  |Q....7..<K..:...|
7F 02 35 02  77 88 D2 A3  04 FD 67 EC  9B 92 B0 83  |..5.w.....g.....|
AB 57                                              |.W              |
Encoded oidDO.typeAttributes.value.direct (CRLContainer):
30 82 03 36  04 04 00 00  00 01 A0 7C  30 7A 31 23  |0..6.......|0z1#|
30 21 06 09  2A 86 48 86  F7 0D 01 09  01 16 14 6D  |0!..*.H........m|
69 76 61 6E  6F 76 40 66  61 63 74 6F  72 2D 74 73  |ivanov@factor-ts|
2E 72 75 31  0B 30 09 06  03 55 04 06  13 02 52 55  |.ru1.0...U....RU|
31 0F 30 0D  06 03 55 04  07 13 06 4D  6F 73 63 6F  |1.0...U....Mosco|
77 31 12 30  10 06 03 55  04 0A 13 09  43 72 79 70  |w1.0...U....Cryp|
74 6F 50 72  6F 31 0E 30  0C 06 03 55  04 0B 13 05  |toPro1.0...U....|
50 72 6F 6D  6F 31 11 30  0F 06 03 55  04 03 13 08  |Promo1.0...U....|
4D 61 78 69  6D 20 55 43  30 82 02 AE  30 82 02 5D  |Maxim UC0...0..]|
02 01 01 30  08 06 06 2A  85 03 02 02  03 30 7A 31  |...0...*.....0z1|
23 30 21 06  09 2A 86 48  86 F7 0D 01  09 01 16 14  |#0!..*.H........|
6D 69 76 61  6E 6F 76 40  66 61 63 74  6F 72 2D 74  |mivanov@factor-t|
73 2E 72 75  31 0B 30 09  06 03 55 04  06 13 02 52  |s.ru1.0...U....R|
55 31 0F 30  0D 06 03 55  04 07 13 06  4D 6F 73 63  |U1.0...U....Mosc|
6F 77 31 12  30 10 06 03  55 04 0A 13  09 43 72 79  |ow1.0...U....Cry|
70 74 6F 50  72 6F 31 0E  30 0C 06 03  55 04 0B 13  |ptoPro1.0...U...|
05 50 72 6F  6D 6F 31 11  30 0F 06 03  55 04 03 13  |.Promo1.0...U...|
08 4D 61 78  69 6D 20 55  43 17 0D 31  32 30 35 31  |.Maxim UC..12051|
35 30 39 31  30 30 36 5A  17 0D 31 32  30 35 32 32  |5091006Z..120522|
32 31 33 30  30 36 5A 30  81 81 30 29  02 0A 61 04  |213006Z0..0)..a.|
D6 67 00 00  00 00 00 12  17 0D 31 32  30 35 30 32  |.g........120502|
31 31 34 31  32 37 5A 30  0C 30 0A 06  03 55 1D 15  |114127Z0.0...U..|
04 03 0A 01  05 30 29 02  0A 61 10 5F  A6 00 00 00  |.....0)..a._....|
00 00 07 17  0D 31 32 30  35 30 32 31  31 33 38 32  |.....120502113 82|
30 5A 30 0C  30 0A 06 03  55 1D 15 04  03 0A 01 05  |0Z0.0...U.......|
30 29 02 0A  61 E9 42 A9  00 00 00 00  00 11 17 0D  |0)..a.B.........|
31 32 30 35  30 32 31 31  33 38 30 35  5A 30 0C 30  |120502113805Z0.0|
0A 06 03 55  1D 15 04 03  0A 01 05 A0  82 01 2E 30  |...U...........0|
82 01 2A 30  1F 06 03 55  1D 23 04 18  30 16 80 14  |..*0...U.#..0...|
C3 99 AC 2E  F8 F6 FC F0  62 2C 8A 80  35 DF DA 63  |........b,..5..c|
28 17 EF ED  30 10 06 09  2B 06 01 04  01 82 37 15  |(...0...+.....7.|
01 04 03 02  01 00 30 0A  06 03 55 1D  14 04 03 02  |......0...U.....|
01 05 30 1C  06 09 2B 06  01 04 01 82  37 15 04 04  |..0...+.....7...|
0F 17 0D 31  32 30 35 32  32 30 39 32  30 30 36 5A  |...120522092006Z|
30 81 CA 06  09 2B 06 01  04 01 82 37  15 0E 04 81  |0....+.....7....|
BC 30 81 B9  30 81 B6 A0  81 B3 A0 81  B0 86 81 AD  |.0..0...........|
6C 64 61 70  3A 2F 2F 2F  43 4E 3D 4D  61 78 69 6D  |ldap:///CN=Maxim|
25 32 30 55  43 2C 43 4E  3D 76 6F 65  6E 6D 65 68  |%20UC,CN=voenmeh|
2D 64 30 66  32 38 36 61  2C 43 4E 3D  43 44 50 2C  |-d0f286a,CN=CDP,|
43 4E 3D 50  75 62 6C 69  63 25 32 30  4B 65 79 25  |CN=Public%20Key%|
32 30 53 65  72 76 69 63  65 73 2C 43  4E 3D 53 65  |20Services,CN=Se|
72 76 69 63  65 73 2C 44  43 3D 55 6E  61 76 61 69  |rvices,DC=Unavai|
6C 61 62 6C  65 43 6F 6E  66 69 67 44  4E 3F 63 65  |lableConfigDN?ce|
72 74 69 66  69 63 61 74  65 52 65 76  6F 63 61 74  |rtificateRevocat|
69 6F 6E 4C  69 73 74 3F  62 61 73 65  3F 6F 62 6A  |ionList?base?obj|
65 63 74 43  6C 61 73 73  3D 63 52 4C  44 69 73 74  |ectClass=cRLDist|
72 69 62 75  74 69 6F 6E  50 6F 69 6E  74 30 08 06  |ributionPoint0..|
06 2A 85 03  02 02 03 03  41 00 70 B6  42 8A 9A E3  |.*......A.p.B...|
05 82 9E 7F  5B 97 A1 6A  B1 84 FB F8  23 E7 F2 CD  |....[..j....#...|
02 A3 02 92  E8 53 83 8F  51 F4 88 A4  0C 37 C6 9D  |.....S..Q....7..|
3C 4B AB 0C  3A A1 0C 0B  7F 02 35 02  77 88 D2 A3  |<K..:.....5.w...|
04 FD 67 EC  9B 92 B0 83  AB 57                    |..g......W      |


Adding token.pkcs15Objects.privateKeys element:

p15_mk_prkey_obj: Making private key 'Private Key of Andrey Fedotov' object:
Choosing PrivateKeyType.privateGostR3410_2001Key choice.
key.commonObjectAttributes.label:
50 72 69 76  61 74 65 20  4B 65 79 20  6F 66 20 41  |Private Key of A|
6E 64 72 65  79 20 46 65  64 6F 74 6F  76           |ndrey Fedotov   |
key.commonObjectAttributes.flags: 0x80, len=1, unused_bits=6
key.classAttributes.iD:
00 00 00 02                                        |....            |
key.classAttributes.usage: len=2, unused_bits=6: 64 40
|d@              |
key.classAttributes.accessFlags: len=1, unused_bits=3: 0xE0
```

```
key.classAttributes.startDate:
32 30 31 32  30 35 31 38  31 31 30 33  30 30 5A     |20120518110300Z |
key.classAttributes.endDate:
32 30 31 33  30 35 31 38  31 31 31 32  30 30 5A     |20130518111200Z |
key.subClassAttributes.subjectName:
30 81 BA 31  23 30 21 06  09 2A 86 48  86 F7 0D 01  |0..1#0!..*.H....|
09 01 16 14  66 65 64 6F  74 6F 76 40  66 61 63 74  |....fedotov@fact|
6F 72 2D 74  73 2E 72 75  31 0B 30 09  06 03 55 04  |or-ts.ru1.0...U.|
06 13 02 52  55 31 15 30  13 06 03 55  04 07 1E 0C  |...RU1.0...U....|
04 1C 04 3E  04 41 04 3A  04 32 04 30  31 1B 30 19  |...>.A.:.2.01.0.|
06 03 55 04  0A 1E 12 04  24 04 30 04  3A 04 42 04  |..U.....$.0.:.B.|
3E 04 40 00  2D 04 22 04  21 31 11 30  0F 06 03 55  |>.@.-.".!1.0...U|
04 0B 1E 08  04 22 04 35  04 41 04 42  31 3F 30 3D  |.....".5.A.B1?0=|
06 03 55 04  03 1E 36 04  24 04 35 04  34 04 3E 04  |..U...6.$.5.4.>.|
42 04 3E 04  32 00 20 04  10 04 3D 04  34 04 40 04  |B.>.2. ...=.4.@.|
35 04 39 00  20 04 12 04  3B 04 30 04  34 04 38 04  |5.9. ...;.0.4.8.|
3C 04 38 04  40 04 3E 04  32 04 38 04  47           |<.8.@.>.2.8.G   |
Encoded GostPrivateKey (98 bytes):
04 60 C5 F7  B3 4F ED A8  10 1D 07 54  A0 07 CD A7  |.`...O.....T....|
57 9F 26 95  D0 B8 54 5D  40 62 C0 B9  EA 51 59 94  |W.&...T]@b...QY.|
19 3B 8D 20  1F 80 E5 92  33 96 41 B7  26 D4 B5 D5  |.;. ....3.A.&...|
26 4A 10 8B  3C A6 64 1F  BB 81 FA 72  96 F5 84 A8  |&J..<.d....r....|
3D B6 4B 4A  FA 0E 9A 4A  0A 83 B4 4F  2E BD 05 F4  |=.KJ...J...O....|
1B C0 70 33  53 F5 CB 5D  5E B1 18 19  3B A4 88 0B  |..p3S..]^...;...|
81 3D                                              |.=              |
Wrapping GostPrivateKey to EnvelopedData (key.typeAttributes.value.direct-protected:
p15_mk_enveloped_data: Making EnvelopedData.recipientInfos (1 kekri):
kekri.kekid.keyIdentifier:
00 00 00 04                                        |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
3F 3B F8 A1  0D 7F B6 83                           |?;......        |
Key wrap:
Pw key:
23 75 43 93  A8 7F 82 88  38 EE 0F D9  17 2D 8C AC  |#uC.....8....-..|
57 E0 66 4F  95 3B 3C 3F  70 EA 72 93  00 0A 8D 88  |W.fO.;<?p.r.....|
Session key:
81 DC A5 40  97 9C 2A 1D  B0 55 FC 32  8F 5E ED 35  |...@..*..U.2.^.5|
12 33 27 2D  0B 18 5C F7  BB 8E 1A 85  98 E0 CA 42  |.3'-..\........B|
Wrapped key:
10 A8 84 C3  2C 16 2F 2F  3E 46 97 D5  45 70 0D 6D  |....,.//>F..Ep.m|
83 AE A3 CB  56 55 D0 C3  75 16 C2 54  2C DA 21 56  |....VU..u..T,.!V|
MAC of key:
37 08 3E 6D                                        |7.>m            |
kekri.encryptedKey content:
30 28 04 20  10 A8 84 C3  2C 16 2F 2F  3E 46 97 D5  |0(. ....,.//>F..|
45 70 0D 6D  83 AE A3 CB  56 55 D0 C3  75 16 C2 54  |Ep.m....VU..u..T|
2C DA 21 56  04 04 37 08  3E 6D                    |,.!V..7.>m      |

EnvelopedData.encryptedContentInfo.contentType: 1.2.840.113549.1.7.1
EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.algorithm: 1.2.643.2.4.3.2.2
Making EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.parameters
(Gost28147_89_Parameters):
par.iv
A3 32 60 BC  E4 20 74 30                           |.2`.. t0        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  A3 32 60 BC  E4 20 74 30  06 07 2A 85  |0....2`.. t0..*.|
03 02 02 1F  01                                    |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
F7 F0 41 FC  C5 14 CB 6D  2A EF A2 5E  D2 D3 17 15  |..A....m*..^....|
DB 96 9B 62  F6 50 20 82  2D 1A 1E AE  CE 3F E4 6F  |...b.P .-....?.o|
41 96 66 68  44 9F B5 A2  98 8F BC AE  61 86 B9 FD  |A.fhD.......a...|
DF F9 81 33  47 08 32 20  0F 7B 4E 18  A0 0C DD 72  |...3G.2 .{N....r|
A9 D2 E8 1E  BB 8A 41 0B  88 EB A8 87  6B 4E 3D 0D  |......A.....kN=.|
46 B2 37 4A  65 00 6D 82  0A D5 52 F3  DA BB 4B 19  |F.7Je.m...R...K.|
09 5E DB 60  F8 CE                                 |.^.`..          |

Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.cryptoProParamSet (1-5 - cproA,B,C,XchA,XchB): 1


Adding token.pkcs15Objects.certificates element:

Making object for certificate 'Certificate of Andrey Fedotov':
Choosing CertificateType.x509Certificate choice.
x509.commonObjectAttributes.label:
```

```
43 65 72 74  69 66 69 63  61 74 65 20  6F 66 20 41  |Certificate of A|
6E 64 72 65  79 20 46 65  64 6F 74 6F  76           |ndrey Fedotov   |
x509.commonObjectAttributes.flags: 0x00, len=1, unused_bits=6
x509.classAttributes.iD:
00 00 00 02                                         |....            |
Choosing x509.typeAttributes.value.direct choice.
Certificate (963 bytes):
30 82 03 BF  30 82 03 6E  A0 03 02 01  02 02 0A 61  |0...0..n.......a|
4A 76 22 00  00 00 00 00  1D 30 08 06  06 2A 85 03  |Jv"......0...*..|
02 02 03 30  7A 31 23 30  21 06 09 2A  86 48 86 F7  |...0z1#0!..*.H..|
0D 01 09 01  16 14 6D 69  76 61 6E 6F  76 40 66 61  |......mivanov@fa|
63 74 6F 72  2D 74 73 2E  72 75 31 0B  30 09 06 03  |ctor-ts.ru1.0...|
55 04 06 13  02 52 55 31  0F 30 0D 06  03 55 04 07  |U....RU1.0...U..|
13 06 4D 6F  73 63 6F 77  31 12 30 10  06 03 55 04  |..Moscow1.0...U.|
0A 13 09 43  72 79 70 74  6F 50 72 6F  31 0E 30 0C  |...CryptoPro1.0.|
06 03 55 04  0B 13 05 50  72 6F 6D 6F  31 11 30 0F  |..U....Promo1.0.|
06 03 55 04  03 13 08 4D  61 78 69 6D  20 55 43 30  |..U....Maxim UC0|
1E 17 0D 31  32 30 35 31  38 31 31 30  33 30 30 5A  |...120518110300Z|
17 0D 31 33  30 35 31 38  31 31 31 32  30 30 5A 30  |..130518111200Z0|
81 BA 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |..1#0!..*.H.....|
01 16 14 66  65 64 6F 74  6F 76 40 66  61 63 74 6F  |...fedotov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 15 30 13  06 03 55 04  07 1E 0C 04  |..RU1.0...U.....|
1C 04 3E 04  41 04 3A 04  32 04 30 31  1B 30 19 06  |..>.A.:.2.01.0..|
03 55 04 0A  1E 12 04 24  04 30 04 3A  04 42 04 3E  |.U.....$.0.:.B.>|
04 40 00 2D  04 22 04 21  31 11 30 0F  06 03 55 04  |.@.-.".!1.0...U.|
0B 1E 08 04  22 04 35 04  41 04 42 31  3F 30 3D 06  |....".5.A.B1?0=.|
03 55 04 03  1E 36 04 24  04 35 04 34  04 3E 04 42  |.U...6.$.5.4.>.B|
04 3E 04 32  00 20 04 10  04 3D 04 34  04 40 04 35  |.>.2. ...=.4.@.5|
04 39 00 20  04 12 04 3B  04 30 04 34  04 38 04 3C  |.9. ...;.0.4.8.<|
04 38 04 40  04 3E 04 32  04 38 04 47  30 63 30 1C  |.8.@.>.2.8.G0c0.|
06 06 2A 85  03 02 02 13  30 12 06 07  2A 85 03 02  |..*.....0...*...|
02 23 01 06  07 2A 85 03  02 02 1E 01  03 43 00 04  |.#...*.......C..|
40 ED 92 03  66 00 10 11  B9 AC 32 68  28 56 76 95  |@...f.....2h(Vv.|
D2 4B B1 1F  22 66 82 FC  53 CC 91 CA  6A 0A 14 30  |.K.."f..S...j..0|
67 27 6A 53  43 D1 E2 93  16 4B 21 00  12 89 47 C8  |g'jSC....K!...G.|
86 F9 21 44  95 51 08 A7  45 E6 17 85  73 75 9D 64  |..!D.Q..E...su.d|
4E A3 82 01  91 30 82 01  8D 30 0E 06  03 55 1D 0F  |N....0...0...U..|
01 01 FF 04  04 03 02 04  F0 30 13 06  03 55 1D 25  |.........0...U.%|
04 0C 30 0A  06 08 2B 06  01 05 05 08  02 02 30 1D  |..0...+.......0.|
06 03 55 1D  0E 04 16 04  14 52 58 AD  0C 45 43 0D  |..U......RX..EC.|
E5 F6 DE 39  7B 77 3B 3D  F9 1D 69 FF  39 30 1F 06  |...9{w;=..i.90..|
03 55 1D 23  04 18 30 16  80 14 C3 99  AC 2E F8 F6  |.U.#..0.........|
FC F0 62 2C  8A 80 35 DF  DA 63 28 17  EF ED 30 75  |..b,..5..c(...0u|
06 03 55 1D  1F 04 6E 30  6C 30 6A A0  68 A0 66 86  |..U...n0l0j.h.f.|
30 68 74 74  70 3A 2F 2F  76 6F 65 6E  6D 65 68 2D  |0http://voenmeh-|
64 30 66 32  38 36 61 2F  43 65 72 74  45 6E 72 6F  |d0f286a/CertEnro|
6C 6C 2F 4D  61 78 69 6D  25 32 30 55  43 2E 63 72  |ll/Maxim%20UC.cr|
6C 86 32 66  69 6C 65 3A  2F 2F 5C 5C  76 6F 65 6E  |l.2file://\\voen|
6D 65 68 2D  64 30 66 32  38 36 61 5C  43 65 72 74  |meh-d0f286a\Cert|
45 6E 72 6F  6C 6C 5C 4D  61 78 69 6D  25 32 30 55  |Enroll\Maxim%20U|
43 2E 63 72  6C 30 81 AE  06 08 2B 06  01 05 05 07  |C.crl0....+.....|
01 01 04 81  A1 30 81 9E  30 4C 06 08  2B 06 01 05  |.....0..0L..+...|
05 07 30 02  86 40 68 74  74 70 3A 2F  2F 76 6F 65  |..0..@http://voe|
6E 6D 65 68  2D 64 30 66  32 38 36 61  2F 43 65 72  |nmeh-d0f286a/Cer|
74 45 6E 72  6F 6C 6C 2F  76 6F 65 6E  6D 65 68 2D  |tEnroll/voenmeh-|
64 30 66 32  38 36 61 5F  4D 61 78 69  6D 25 32 30  |d0f286a_Maxim%20|
55 43 2E 63  72 74 30 4E  06 08 2B 06  01 05 05 07  |UC.crt0N..+.....|
30 02 86 42  66 69 6C 65  3A 2F 2F 5C  5C 76 6F 65  |0..Bfile://\\voe|
6E 6D 65 68  2D 64 30 66  32 38 36 61  5C 43 65 72  |nmeh-d0f286a\Cer|
74 45 6E 72  6F 6C 6C 5C  76 6F 65 6E  6D 65 68 2D  |tEnroll\voenmeh-|
64 30 66 32  38 36 61 5F  4D 61 78 69  6D 25 32 30  |d0f286a_Maxim%20|
55 43 2E 63  72 74 30 08  06 06 2A 85  03 02 02 03  |UC.crt0...*.....|
03 41 00 71  DB 23 67 25  9C C9 D0 86  2A C9 1D D9  |.A.q.#g%....*...|
9D AA C8 51  BC A9 2C BA  F4 82 F3 F4  8E CF 0C 81  |...Q..,.........|
77 A7 2F 35  34 8A D8 9B  B1 B0 0A 18  50 A2 7E CF  |w./54.......P.~.|
8A 6D CB 5E  53 21 88 08  EC F3 CA 7A  36 02 8D A2  |.m.^S!.....z6...|
F1 F5 E4                                            |...             |
x509.typeAttributes.subject:
30 81 BA 31  23 30 21 06  09 2A 86 48  86 F7 0D 01  |0..1#0!..*.H....|
09 01 16 14  66 65 64 6F  74 6F 76 40  66 61 63 74  |....fedotov@fact|
6F 72 2D 74  73 2E 72 75  31 0B 30 09  06 03 55 04  |or-ts.ru1.0...U.|
06 13 02 52  55 31 15 30  13 06 03 55  04 07 1E 0C  |...RU1.0...U....|
04 1C 04 3E  04 41 04 3A  04 32 04 30  31 1B 30 19  |...>.A.:.2.01.0.|
06 03 55 04  0A 1E 12 04  24 04 30 04  3A 04 42 04  |..U.....$.0.:.B.|
3E 04 40 00  2D 04 22 04  21 31 11 30  0F 06 03 55  |>.@.-.".!1.0...U|
04 0B 1E 08  04 22 04 35  04 41 04 42  31 3F 30 3D  |.....".5.A.B1?0=|
06 03 55 04  03 1E 36 04  24 04 35 04  34 04 3E 04  |..U...6.$.5.4.>.|
42 04 3E 04  32 00 20 04  10 04 3D 04  34 04 40 04  |B.>.2. ...=.4.@.|
```

```
35 04 39 00  20 04 12 04  3B 04 30 04  34 04 38 04  |5.9. ...;.0.4.8.|
3C 04 38 04  40 04 3E 04  32 04 38 04  47           |<.8.@.>.2.8.G   |
x509.typeAttributes.issuer:
30 7A 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |0z1#0!..*.H.....|
01 16 14 6D  69 76 61 6E  6F 76 40 66  61 63 74 6F  |...mivanov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 0F 30 0D  06 03 55 04  07 13 06 4D  |..RU1.0...U....M|
6F 73 63 6F  77 31 12 30  10 06 03 55  04 0A 13 09  |oscow1.0...U....|
43 72 79 70  74 6F 50 72  6F 31 0E 30  0C 06 03 55  |CryptoPro1.0...U|
04 0B 13 05  50 72 6F 6D  6F 31 11 30  0F 06 03 55  |....Promo1.0...U|
04 03 13 08  4D 61 78 69  6D 20 55 43               |....Maxim UC    |


Adding token.pkcs15Objects.privateKeys element:

p15_mk_prkey_obj: Making private key 'New Generated Private Key' object:
Choosing PrivateKeyType.privateGostR3410_2001Key choice.
key.commonObjectAttributes.label:
4E 65 77 20  47 65 6E 65  72 61 74 65  64 20 50 72  |New Generated Pr|
69 76 61 74  65 20 4B 65  79                       |ivate Key       |
key.commonObjectAttributes.flags: 0x80, len=1, unused_bits=6
key.classAttributes.iD:
00 00 00 03                                        |....            |
key.classAttributes.usage: len=2, unused_bits=6: 20
|               |
key.classAttributes.accessFlags: len=1, unused_bits=3: 0xE0
Encoded GostPrivateKey (98 bytes):
04 60 09 31  E6 3C BD 14  0A F3 29 65  47 A6 93 2A  |.`.1.<....)eG..*|
01 AC 32 7B  B3 01 6D ED  53 77 CB 1C  3B 5F 02 FD  |..2{..m.Sw..;_..|
CE 12 B7 6D  E5 26 5C 83  3F 86 AC BD  BE D5 AE C1  |...m.&\.?.......|
F1 92 DD 63  D8 78 B8 0D  6A D9 97 2D  4B 2C 20 E7  |...c.x..j..-K, .|
72 2E ED 67  60 4F 56 32  EF 45 7F 4F  91 80 45 4A  |r..g`OV2.E.O..EJ|
DF 7F FB 4C  B9 16 21 7C  F2 EF BB 1A  73 09 78 B0  |...L..!|....s.x.|
9B BA                                              |..              |
Wrapping GostPrivateKey to EnvelopedData (key.typeAttributes.value.direct-protected:
p15_mk_enveloped_data: Making EnvelopedData.recipientInfos (1 kekri):
kekri.kekid.keyIdentifier:
00 00 00 04                                        |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
26 30 47 72  9C E3 74 6F                           |&0Gr..to        |
Key wrap:
Pw key:
23 75 43 93  A8 7F 82 88  38 EE 0F D9  17 2D 8C AC  |#uC.....8....-..|
57 E0 66 4F  95 3B 3C 3F  70 EA 72 93  00 0A 8D 88  |W.fO.;<?p.r.....|
Session key:
AD 59 2B 31  E3 50 A7 85  E9 94 C1 81  11 AA E5 87  |.Y+1.P..........|
BD 9C 9D B9  14 48 6B 3B  86 FA 04 CC  0B EE 5F 8A  |.....Hk;......_.|
Wrapped key:
D6 B9 95 95  DD 7A D6 C3  E6 7D FC 52  19 6E C6 35  |.....z...}.R.n.5|
4E 3E 95 0B  DE 23 C1 23  CB 76 61 98  E4 2E 75 19  |N>...#.#.va...u.|
MAC of key:
FD B5 BD 92                                        |....            |
kekri.encryptedKey content:
30 28 04 20  D6 B9 95 95  DD 7A D6 C3  E6 7D FC 52  |0(. .....z...}.R|
19 6E C6 35  4E 3E 95 0B  DE 23 C1 23  CB 76 61 98  |.n.5N>...#.#.va.|
E4 2E 75 19  04 04 FD B5  BD 92                    |..u.......      |

EnvelopedData.encryptedContentInfo.contentType: 1.2.840.113549.1.7.1
EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.algorithm: 1.2.643.2.4.3.2.2
Making EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.parameters
(Gost28147_89_Parameters):
par.iv
64 59 E7 C7  14 DE 0A E3                           |dY......        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  64 59 E7 C7  14 DE 0A E3  06 07 2A 85  |0...dY........*.|
03 02 02 1F  01                                    |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
17 FA 51 6A  7E 0C 59 F3  E8 72 F0 7B  8D BE 3D F1  |..Qj~.Y..r.{..=.|
D6 76 CF D1  18 C9 00 7D  B1 90 77 E4  6F 68 10 27  |.v.....}..w.oh.'|
D4 5D 11 A4  8E 75 C1 20  DB 9C 73 A4  8A 93 3C EA  |.]...u. ..s...<.|
26 9E CF 3E  06 41 E6 02  C4 0B B6 C9  CD 05 06 4E  |&..>.A.........N|
B5 2B 12 74  09 BE 45 4D  E2 98 8C CF  66 FC 5F 57  |.+.t..EM....f._W|
07 3D B2 41  8B B9 B6 85  FE 0F D4 7F  7B D2 E0 EF  |.=.A........{...|
32 2C 62 83  F4 07                                 |2,b...          |
```

```
Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.cryptoProParamSet (1-5 - cproA,B,C,XchA,XchB): 2


Adding token.pkcs15Objects.publicKeys element:

p15_mk_pubkey_obj: Making public key 'Public Key for New Generated Private Key' object:
Choosing PublicKeyType.publicGostR3410_2001Key choice.
key.commonObjectAttributes.label:
50 75 62 6C  69 63 20 4B  65 79 20 66  6F 72 20 4E  |Public Key for N|
65 77 20 47  65 6E 65 72  61 74 65 64  20 50 72 69  |ew Generated Pri|
76 61 74 65  20 4B 65 79                             |vate Key        |
key.commonObjectAttributes.flags: 0x00, len=1, unused_bits=6
key.classAttributes.iD:
00 00 00 03                                           |....            |
key.classAttributes.usage: len=2, unused_bits=6: 02
|.               |
Making key.typeAttributes.value:
Choosing key.typeAttributes.value.direct.raw choice.
GostR3410-2001Point (w/o ostr header):
1E 8B CE FD  7C 95 E8 4F  11 E3 5A 14  A0 58 FD 5B  |....|..O..Z..X.[|
CB 3E 24 89  3A DE 91 59  99 EB 27 5B  A3 AF AF 1D  |.>$.:..Y..'[....|
D4 D5 8D 6C  32 A2 64 D3  8A E6 CD 07  54 0C 76 7B  |...l2.d.....T.v{|
41 5E 64 54  0B E9 23 02  A7 F4 EA FA  65 CD F6 4B  |A^dT..#.....e..K|
Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.cryptoProParamSet (1-5 - cproA,B,C,XchA,XchB): 2


Adding token.pkcs15Objects.dataObjects (abstract data) element:

Making abstract data object 'Top-secret Data'
Choosing DataType.oidDO choice.
oidDO.commonObjectAttributes.label:
54 6F 70 2D  73 65 63 72  65 74 20 44  61 74 61      |Top-secret Data |
oidDO.commonObjectAttributes.flags: 0xC0, len=1, unused_bits=6
oidDO.classAttributes.applicationOID: 1.3.6.1.4.1.13312.503.1.4
oidDO.typeAttributes.id: 1.1.456.7890
Choosing oidDO.typeAttributes.value.direct-protected choice.
Data to encrypt (wrapped in OCTET STRING): (82 bytes):
04 50 54 68  69 73 20 69  73 20 73 6F  6D 65 20 63  |.PThis is some c|
6F 6E 66 69  64 65 6E 74  69 61 6C 20  61 62 73 74  |onfidential abst|
72 61 63 74  20 64 61 74  61 2E 20 49  74 20 77 69  |ract data. It wi|
6C 6C 20 62  65 20 65 6E  63 72 79 70  74 65 64 20  |ll be encrypted |
69 6E 20 74  68 65 20 63  6F 6E 74 61  69 6E 65 72  |in the container|
2E 00                                                 |..              |
Wrapping the data to EnvelopedData (oidDO.typeAttributes.value.direct-protected):
p15_mk_enveloped_data: Making EnvelopedData.recipientInfos (1 kekri):
kekri.kekid.keyIdentifier:
00 00 00 04                                           |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
72 1F F5 35  95 22 EC C2                              |r..5."..        |
Key wrap:
Pw key:
23 75 43 93  A8 7F 82 88  38 EE 0F D9  17 2D 8C AC  |#uC.....8....-..|
57 E0 66 4F  95 3B 3C 3F  70 EA 72 93  00 0A 8D 88  |W.fO.;<?p.r.....|
Session key:
54 9B A9 4A  DD EF B9 F6  6F 33 A1 47  8D CF B8 FF  |T..J....o3.G....|
E5 16 96 F1  B7 92 CE CB  37 07 FF 0B  FB 99 D3 71  |........7......q|
Wrapped key:
F2 D2 EE E6  12 44 64 20  97 1F 02 A7  D2 0C C5 D5  |.....Dd ........|
77 46 96 F0  3D F8 B5 62  3D A9 45 0A  E6 DF 6D 64  |wF..=..b=.E...md|
MAC of key:
E2 0A 7F 02                                           |....            |
kekri.encryptedKey content:
30 28 04 20  F2 D2 EE E6  12 44 64 20  97 1F 02 A7  |0(. .....Dd ....|
D2 0C C5 D5  77 46 96 F0  3D F8 B5 62  3D A9 45 0A  |....wF..=..b=.E.|
E6 DF 6D 64  04 04 E2 0A  7F 02                       |..md......      |

EnvelopedData.encryptedContentInfo.contentType: 1.2.840.113549.1.7.1
EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.algorithm: 1.2.643.2.4.3.2.2
Making EnvelopedData.encryptedContentInfo.contentEncryptionAlgorithm.parameters
(Gost28147_89_Parameters):
par.iv
3F 90 96 7B  F8 3F 30 1D                              |?..{.?0.        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  3F 90 96 7B  F8 3F 30 1D  06 07 2A 85  |0...?..{.?0...*.|
```

```
03 02 02 1F  01                                        |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
15 9D C1 8F  62 07 70 D0  03 31 74 DF  A7 02 5C D9  |....b.p..1t...\.|
22 3C F2 97  AA D5 D4 F1  C5 E7 06 04  64 F9 73 2E  |"<..........d.s.|
64 B4 5B C2  50 4A 52 64  B0 A9 FB 07  27 F5 37 58  |d.[.PJRd....'.7X|
EF 4D B0 BD  A3 69 A1 A8  77 2C 15 25  8E 50 07 8F  |.M...i..w,.%.P..|
E0 CA 14 EF  F6 3A C1 16  19 76 C9 31  DB A3 37 6D  |.....:...v.1..7m|
96 F6 8C 81  6B 68                                  |....kh          |


Adding token.pkcs15Objects.dataObjects (abstract data) element:

Making abstract data object 'Public Data'
Choosing DataType.oidDO choice.
oidDO.commonObjectAttributes.label:
50 75 62 6C  69 63 20 44  61 74 61                  |Public Data     |
oidDO.commonObjectAttributes.flags: 0x40, len=1, unused_bits=6
oidDO.classAttributes.applicationOID: 1.3.6.1.4.1.13312.503.1.4
oidDO.typeAttributes.id: 1.1.765.432.1
Choosing oidDO.typeAttributes.value.direct choice.
Data (wrapped in OCTET STRING) oidDO.typeAttributes.value.direct:
04 37 54 68  69 73 20 69  73 20 73 6F  6D 65 20 6F  |.7This is some o|
70 65 6E 20  64 61 74 61  2E 20 54 68  65 72 65 27  |pen data. There'|
73 20 6E 6F  20 6E 65 65  64 20 74 6F  20 65 6E 63  |s no need to enc|
72 79 70 74  20 69 74 2E  00                        |rypt it..       |


AuthenticatedData.encapContentInfo.eContent (w/o ostr header) (5154 bytes):
30 82 14 1E  02 01 00 A0  4C 30 4A 04  04 00 00 00  |0.......L0J.....|
04 A0 42 30  40 06 09 2A  86 48 86 F7  0D 01 05 0C  |..B0@..*.H......|
30 33 04 20  F4 53 80 45  B0 2F C8 C6  DE AA 01 ED  |03. .S.E./......|
A5 16 21 DD  B1 65 FB 1F  53 AB C9 4C  1D 64 B3 BD  |..!..e..S..L.d..|
3F D9 D8 0C  02 02 07 D0  02 01 20 30  08 06 06 2A  |?......... 0...*|
85 03 02 02  0A 30 82 13  C9 A7 82 01  6D A0 82 01  |.....0......m...|
69 A1 40 30  16 0C 11 46  61 63 74 6F  72 2D 54 53  |i.@0...Factor-TS|
20 76 65 72  73 69 6F 6E  03 01 00 30  0D 06 0B 2B  | version...0...+|
06 01 04 01  E8 00 83 77  01 03 A1 17  06 0B 2B 06  |.......w......+.|
01 04 01 E8  00 83 77 01  03 A0 08 30  06 02 01 02  |......w....0....|
80 01 00 A1  82 01 23 30  17 0C 11 52  61 6E 64 6F  |......#0...Rando|
6D 20 49 6E  69 74 20 56  61 6C 75 65  03 02 06 C0  |m Init Value....|
30 0D 06 0B  2B 06 01 04  01 E8 00 83  77 01 01 A1  |0...+.......w...|
81 F8 06 0B  2B 06 01 04  01 E8 00 83  77 01 01 A2  |....+.......w...|
81 E8 02 01  02 31 59 A2  57 02 01 04  30 06 04 04  |.....1Y.W...0...|
00 00 00 04  30 1E 06 07  2A 85 03 02  02 0D 01 30  |....0...*......0|
13 06 07 2A  85 03 02 02  1F 01 04 08  74 70 70 52  |...*........tppR|
12 2A 80 50  04 2A 30 28  04 20 5D 7F  85 0F 18 0A  |.*.P.*0(. ].....|
20 A5 FA 27  BC D4 13 77  39 AF A3 51  DB E7 3C B3  | ..'...w9..Q..<.|
88 80 BB BE  B8 41 5B 42  46 28 04 04  5A 69 79 CD  |.....A[BF(..Ziy.|
30 81 87 06  09 2A 86 48  86 F7 0D 01  07 01 30 1F  |0....*.H......0.|
06 08 2A 85  03 02 04 03  02 02 30 13  04 08 DD 8E  |..*.......0.....|
C8 00 0F CA  11 88 06 07  2A 85 03 02  02 1F 01 80  |........*.......|
59 93 9B 98  38 70 4A 73  DD A0 AE AF  87 4C 4A 00  |Y...8pJs.....LJ.|
AD 62 B8 21  AA 5C 89 C2  FF 92 1C 5C  43 40 54 BC  |.b.!.\.....\C@T.|
B6 AA 28 D3  14 8B E9 6F  62 F2 06 37  69 25 2C 5D  |..(....ob..7i%,]|
09 C9 26 44  14 23 51 85  DD 99 06 95  02 8E 0B 98  |..&D.#Q.........|
BE F5 46 55  CF 63 D8 E5  48 7D 63 25  75 2B F4 B1  |..FU.c..H}c%u+..|
93 E6 3E 22  AA DB DC 46  03 91 A5 82  03 FD A0 82  |..>"...F........|
03 F9 30 82  03 F5 30 1B  0C 16 52 6F  6F 74 20 43  |..0...0...Root C|
65 72 74 69  66 69 63 61  74 65 20 6F  66 20 43 41  |ertificate of CA|
03 01 00 30  09 04 04 00  00 00 01 01  01 FF A1 82  |...0............|
03 C9 A0 82  02 B9 30 82  02 68 A0 03  02 01 02 02  |......0..h......|
10 07 48 BA  C5 90 EA C5  9B 4C 4F 0F  E7 04 98 9C  |..H......LO.....|
A8 30 08 06  06 2A 85 03  02 02 03 30  7A 31 23 30  |.0...*.....0z1#0|
21 06 09 2A  86 48 86 F7  0D 01 09 01  16 14 6D 69  |!..*.H........mi|
76 61 6E 6F  76 40 66 61  63 74 6F 72  2D 74 73 2E  |vanov@factor-ts.|
72 75 31 0B  30 09 06 03  55 04 06 13  02 52 55 31  |ru1.0...U....RU1|
0F 30 0D 06  03 55 04 07  13 06 4D 6F  73 63 6F 77  |.0...U....Moscow|
31 12 30 10  06 03 55 04  0A 13 09 43  72 79 70 74  |1.0...U....Crypt|
6F 50 72 6F  31 0E 30 0C  06 03 55 04  0B 13 05 50  |oPro1.0...U....P|
72 6F 6D 6F  31 11 30 0F  06 03 55 04  03 13 08 4D  |romo1.0...U....M|
61 78 69 6D  20 55 43 30  1E 17 0D 31  32 30 33 32  |axim UC0...12032|
31 31 32 33  39 33 38 5A  17 0D 31 37  30 33 32 31  |1123938Z..170321|
31 32 34 36  31 32 5A 30  7A 31 23 30  21 06 09 2A  |124612Z0z1#0!..*|
86 48 86 F7  0D 01 09 01  16 14 6D 69  76 61 6E 6F  |.H........mivano|
76 40 66 61  63 74 6F 72  2D 74 73 2E  72 75 31 0B  |v@factor-ts.ru1.|
30 09 06 03  55 04 06 13  02 52 55 31  0F 30 0D 06  |0...U....RU1.0..|
03 55 04 07  13 06 4D 6F  73 63 6F 77  31 12 30 10  |.U....Moscow1.0.|
06 03 55 04  0A 13 09 43  72 79 70 74  6F 50 72 6F  |..U....CryptoPro|
```

```
31 0E 30 0C  06 03 55 04  0B 13 05 50  72 6F 6D 6F  |1.0...U....Promo|
31 11 30 0F  06 03 55 04  03 13 08 4D  61 78 69 6D  |1.0...U....Maxim|
20 55 43 30  63 30 1C 06  06 2A 85 03  02 02 13 30  | UC0c0...*.....0|
12 06 07 2A  85 03 02 02  23 01 06 07  2A 85 03 02  |...*....#...*...|
02 1E 01 03  43 00 04 40  97 CB DD 42  DF 80 28 13  |....C..@...B..(.|
B2 99 11 64  6B E1 38 12  02 1F 6E 83  5F B3 35 B1  |...dk.8...n._.5.|
48 15 E0 43  CD 76 24 6D  8D 70 52 10  B8 61 47 40  |H..C.v$m.pR..aG@|
CF E2 31 4E  54 51 39 D5  CF 23 BB 24  47 59 27 2F  |..1NTQ9..#.$GY'/|
D7 9D F4 42  A8 C4 DD 9C  A3 81 C7 30  81 C4 30 0B  |...B.......0..0.|
06 03 55 1D  0F 04 04 03  02 01 86 30  0F 06 03 55  |..U........0...U|
1D 13 01 01  FF 04 05 30  03 01 01 FF  30 1D 06 03  |.......0....0...|
55 1D 0E 04  16 04 14 C3  99 AC 2E F8  F6 FC F0 62  |U..............b|
2C 8A 80 35  DF DA 63 28  17 EF ED 30  73 06 03 55  |,..5..c(...0s..U|
1D 1F 04 6C  30 6A 30 68  A0 66 A0 64  86 30 68 74  |...l0j0h.f.d.0ht|
74 70 3A 2F  2F 76 6F 65  6E 6D 65 68  2D 64 30 66  |tp://voenmeh-d0f|
32 38 36 61  2F 43 65 72  74 45 6E 72  6F 6C 6C 2F  |286a/CertEnroll/|
4D 61 78 69  6D 25 32 30  55 43 2E 63  72 6C 86 30  |Maxim%20UC.crl.0|
66 69 6C 65  3A 2F 2F 5C  5C 76 6F 65  6E 6D 65 68  |file://\\voenmeh|
2D 64 30 66  32 38 36 61  5C 43 65 72  74 45 6E 72  |-d0f286a\CertEnr|
6F 6C 6C 5C  4D 61 78 69  6D 20 55 43  2E 63 72 6C  |oll\Maxim UC.crl|
30 10 06 09  2B 06 01 04  01 82 37 15  01 04 03 02  |0...+.....7.....|
01 00 30 08  06 06 2A 85  03 02 02 03  03 41 00 C1  |..0...*......A..|
74 E0 FC 28  6F 84 9C BA  FA 24 ED A3  AB D1 44 97  |t..(o....$....D.|
D4 E2 46 74  C2 D4 9E B9  F8 1B 53 1C  98 BA AA 95  |..Ft......S.....|
DB EB DA 76  A2 45 2F 05  99 F1 96 B3  9F 2F F1 71  |...v.E/....../.q|
E5 12 66 CB  EB 59 39 32  F5 7B 6A D0  7C F8 AD 30  |..f..Y92.{j.|..0|
7A 31 23 30  21 06 09 2A  86 48 86 F7  0D 01 09 01  |z1#0!..*.H......|
16 14 6D 69  76 61 6E 6F  76 40 66 61  63 74 6F 72  |..mivanov@factor|
2D 74 73 2E  72 75 31 0B  30 09 06 03  55 04 06 13  |-ts.ru1.0...U...|
02 52 55 31  0F 30 0D 06  03 55 04 07  13 06 4D 6F  |.RU1.0...U....Mo|
73 63 6F 77  31 12 30 10  06 03 55 04  0A 13 09 43  |scow1.0...U....C|
72 79 70 74  6F 50 72 6F  31 0E 30 0C  06 03 55 04  |ryptoPro1.0...U.|
0B 13 05 50  72 6F 6D 6F  31 11 30 0F  06 03 55 04  |...Promo1.0...U.|
03 13 08 4D  61 78 69 6D  20 55 43 A0  7C 30 7A 31  |...Maxim UC.|0z1|
23 30 21 06  09 2A 86 48  86 F7 0D 01  09 01 16 14  |#0!..*.H........|
6D 69 76 61  6E 6F 76 40  66 61 63 74  6F 72 2D 74  |mivanov@factor-t|
73 2E 72 75  31 0B 30 09  06 03 55 04  06 13 02 52  |s.ru1.0...U....R|
55 31 0F 30  0D 06 03 55  04 07 13 06  4D 6F 73 63  |U1.0...U....Mosc|
6F 77 31 12  30 10 06 03  55 04 0A 13  09 43 72 79  |ow1.0...U....Cry|
70 74 6F 50  72 6F 31 0E  30 0C 06 03  55 04 0B 13  |ptoPro1.0...U...|
05 50 72 6F  6D 6F 31 11  30 0F 06 03  55 04 03 13  |.Promo1.0...U...|
08 4D 61 78  69 6D 20 55  43 02 10 07  48 BA C5 90  |.Maxim UC...H...|
EA C5 9B 4C  4F 0F E7 04  98 9C A8 A7  82 03 78 A0  |...LO.........x.|
82 03 74 A1  82 03 70 30  10 0C 0B 43  52 4C 20 66  |..t...p0...CRL f|
72 6F 6D 20  43 41 03 01  00 30 0D 06  0B 2B 06 01  |rom CA...0...+..|
04 01 E8 00  83 77 01 02  A1 82 03 4B  06 0B 2B 06  |.....w.....K..+.|
01 04 01 E8  00 83 77 01  02 A0 82 03  3A 30 82 03  |......w.....:0..|
36 04 04 00  00 00 01 A0  7C 30 7A 31  23 30 21 06  |6.......|0z1#0!.|
09 2A 86 48  86 F7 0D 01  09 01 16 14  6D 69 76 61  |.*.H........miva|
6E 6F 76 40  66 61 63 74  6F 72 2D 74  73 2E 72 75  |nov@factor-ts.ru|
31 0B 30 09  06 03 55 04  06 13 02 52  55 31 0F 30  |1.0...U....RU1.0|
0D 06 03 55  04 07 13 06  4D 6F 73 63  6F 77 31 12  |...U....Moscow1.|
30 10 06 03  55 04 0A 13  09 43 72 79  70 74 6F 50  |0...U....CryptoP|
72 6F 31 0E  30 0C 06 03  55 04 0B 13  05 50 72 6F  |ro1.0...U....Pro|
6D 6F 31 11  30 0F 06 03  55 04 03 13  08 4D 61 78  |mo1.0...U....Max|
69 6D 20 55  43 30 82 02  AE 30 82 02  5D 02 01 01  |im UC0...0..]...|
30 08 06 06  2A 85 03 02  02 03 30 7A  31 23 30 21  |0...*.....0z1#0!|
06 09 2A 86  48 86 F7 0D  01 09 01 16  14 6D 69 76  |..*.H........miv|
61 6E 6F 76  40 66 61 63  74 6F 72 2D  74 73 2E 72  |anov@factor-ts.r|
75 31 0B 30  09 06 03 55  04 06 13 02  52 55 31 0F  |u1.0...U....RU1.|
30 0D 06 03  55 04 07 13  06 4D 6F 73  63 6F 77 31  |0...U....Moscow1|
12 30 10 06  03 55 04 0A  13 09 43 72  79 70 74 6F  |.0...U....Crypto|
50 72 6F 31  0E 30 0C 06  03 55 04 0B  13 05 50 72  |Pro1.0...U....Pr|
6F 6D 6F 31  11 30 0F 06  03 55 04 03  13 08 4D 61  |omo1.0...U....Ma|
78 69 6D 20  55 43 17 0D  31 32 30 35  31 35 30 39  |xim UC..12051509|
31 30 30 36  5A 17 0D 31  32 30 35 32  32 32 31 33  |1006Z..120522213|
30 30 36 5A  30 81 81 30  29 02 0A 61  04 D6 67 00  |006Z0..0)..a..g.|
00 00 00 00  12 17 0D 31  32 30 35 30  32 31 31 34  |.......120502114|
31 32 37 5A  30 0C 30 0A  06 03 55 1D  15 04 03 0A  |127Z0.0...U.....|
01 05 30 29  02 0A 61 10  5F A6 00 00  00 00 00 07  |..0)..a._.......|
17 0D 31 32  30 35 30 32  31 31 33 38  32 30 5A 30  |..120502113820Z0|
0C 30 0A 06  03 55 1D 15  04 03 0A 01  05 30 29 02  |.0...U.......0).|
0A 61 E9 42  A9 00 00 00  00 00 11 17  0D 31 32 30  |.a.B.........120|
35 30 32 31  31 33 38 30  35 5A 30 0C  30 0A 06 03  |502113805Z0.0...|
55 1D 15 04  03 0A 01 05  A0 82 01 2E  30 82 01 2A  |U...........0..*|
30 1F 06 03  55 1D 23 04  18 30 16 80  14 C3 99 AC  |0...U.#..0......|
2E F8 F6 FC  F0 62 2C 8A  80 35 DF DA  63 28 17 EF  |.....b,..5..c(..|
ED 30 10 06  09 2B 06 01  04 01 82 37  15 01 04 03  |.0...+.....7....|
02 01 00 30  0A 06 03 55  1D 14 04 03  02 01 05 30  |...0...U.......0|
```

```
1C 06 09 2B  06 01 04 01  82 37 15 04  04 0F 17 0D  |...+.....7......|
31 32 30 35  32 32 30 39  32 30 30 36  5A 30 81 CA  |120522092006Z0..|
06 09 2B 06  01 04 01 82  37 15 0E 04  81 BC 30 81  |..+.....7.....0.|
B9 30 81 B6  A0 81 B3 A0  81 B0 86 81  AD 6C 64 61  |.0...........lda|
70 3A 2F 2F  2F 43 4E 3D  4D 61 78 69  6D 25 32 30  |p:///CN=Maxim%20|
55 43 2C 43  4E 3D 76 6F  65 6E 6D 65  68 2D 64 30  |UC,CN=voenmeh-d0|
66 32 38 36  61 2C 43 4E  3D 43 44 50  2C 43 4E 3D  |f286a,CN=CDP,CN=|
50 75 62 6C  69 63 25 32  30 4B 65 79  25 32 30 53  |Public%20Key%20S|
65 72 76 69  63 65 73 2C  43 4E 3D 53  65 72 76 69  |ervices,CN=Servi|
63 65 73 2C  44 43 3D 55  6E 61 76 61  69 6C 61 62  |ces,DC=Unavailab|
6C 65 43 6F  6E 66 69 67  44 4E 3F 63  65 72 74 69  |leConfigDN?certi|
66 69 63 61  74 65 52 65  76 6F 63 61  74 69 6F 6E  |ficateRevocation|
4C 69 73 74  3F 62 61 73  65 3F 6F 62  6A 65 63 74  |List?base?object|
43 6C 61 73  73 3D 63 52  4C 44 69 73  74 72 69 62  |Class=cRLDistrib|
75 74 69 6F  6E 50 6F 69  6E 74 30 08  06 06 2A 85  |utionPoint0...*.|
03 02 02 03  03 41 00 70  B6 42 8A 9A  E3 05 82 9E  |.....A.p.B......|
7F 5B 97 A1  6A B1 84 FB  F8 23 E7 F2  CD 02 A3 02  |.[..j....#......|
92 E8 53 83  8F 51 F4 88  A4 0C 37 C6  9D 3C 4B AB  |..S..Q....7..<K.|
0C 3A A1 0C  0B 7F 02 35  02 77 88 D2  A3 04 FD 67  |.:.....5.w.....g|
EC 9B 92 B0  83 AB 57 A0  82 02 27 A0  82 02 23 BA  |......W...'...#.|
82 02 1F 30  23 0C 1D 50  72 69 76 61  74 65 20 4B  |...0#..Private K|
65 79 20 6F  66 20 41 6E  64 72 65 79  20 46 65 64  |ey of Andrey Fed|
6F 74 6F 76  03 02 07 80  30 31 04 04  00 00 00 02  |otov....01......|
03 03 06 64  40 03 02 05  E0 18 0F 32  30 31 32 30  |...d@......20120|
35 31 38 31  31 30 33 30  30 5A 80 0F  32 30 31 33  |518110300Z..2013|
30 35 31 38  31 31 31 32  30 30 5A A0  81 BD 30 81  |0518111200Z...0.|
BA 31 23 30  21 06 09 2A  86 48 86 F7  0D 01 09 01  |.1#0!..*.H......|
16 14 66 65  64 6F 74 6F  76 40 66 61  63 74 6F 72  |..fedotov@factor|
2D 74 73 2E  72 75 31 0B  30 09 06 03  55 04 06 13  |-ts.ru1.0...U...|
02 52 55 31  15 30 13 06  03 55 04 07  1E 0C 04 1C  |.RU1.0...U......|
04 3E 04 41  04 3A 04 32  04 30 31 1B  30 19 06 03  |.>.A.:.2.01.0...|
55 04 0A 1E  12 04 24 04  30 04 3A 04  42 04 3E 04  |U.....$.0.:.B.>.|
40 00 2D 04  22 04 21 31  11 30 0F 06  03 55 04 0B  |@.-."."!1.0...U..|
1E 08 04 22  04 35 04 41  04 42 31 3F  30 3D 06 03  |..."5.A.B1?0=..|
55 04 03 1E  36 04 24 04  35 04 34 04  3E 04 42 04  |U...6.$.5.4.>.B.|
3E 04 32 00  20 04 10 04  3D 04 34 04  40 04 35 04  |>.2. ...=.4.@.5.|
39 00 20 04  12 04 3B 04  30 04 34 04  38 04 3C 04  |9. ...;.0.4.8.<.|
38 04 40 04  3E 04 32 04  38 04 47 A1  82 01 03 A2  |8.@.>.2.8.G.....|
81 F5 02 01  02 31 59 A2  57 02 01 04  30 06 04 04  |.....1Y.W...0...|
00 00 00 04  30 1E 06 07  2A 85 03 02  02 0D 01 30  |....0...*......0|
13 06 07 2A  85 03 02 02  1F 01 04 08  3F 3B F8 A1  |...*........?;..|
0D 7F B6 83  04 2A 30 28  04 20 10 A8  84 C3 2C 16  |.....*0(. ....,.|
2F 2F 3E 46  97 D5 45 70  0D 6D 83 AE  A3 CB 56 55  |//>F..Ep.m....VU|
D0 C3 75 16  C2 54 2C DA  21 56 04 04  37 08 3E 6D  |..u..T,.!V..7.>m|
30 81 94 06  09 2A 86 48  86 F7 0D 01  07 01 30 1F  |0....*.H......0.|
06 08 2A 85  03 02 04 03  02 02 30 13  04 08 A3 32  |..*.......0....2|
60 BC E4 20  74 30 06 07  2A 85 03 02  02 1F 01 80  |`.. t0..*.......|
66 F7 F0 41  FC C5 14 CB  6D 2A EF A2  5E D2 D3 17  |f..A....m*..^...|
15 DB 96 9B  62 F6 50 20  82 2D 1A 1E  AE CE 3F E4  |....b.P .-....?.|
6F 41 96 66  68 44 9F B5  A2 98 8F BC  AE 61 86 B9  |oA.fhD.......a..|
FD DF F9 81  33 47 08 32  20 0F 7B 4E  18 A0 0C DD  |....3G.2 .{N....|
72 A9 D2 E8  1E BB 8A 41  0B 88 EB A8  87 6B 4E 3D  |r......A.....kN=|
0D 46 B2 37  4A 65 00 6D  82 0A D5 52  F3 DA BB 4B  |.F.7Je.m...R...K|
19 09 5E DB  60 F8 CE 30  09 06 07 2A  85 03 02 02  |..^.`..0...*....|
23 01 A4 82  05 42 A0 82  05 3E 30 82  05 3A 30 22  |#....B...>0..:0"|
0C 1D 43 65  72 74 69 66  69 63 61 74  65 20 6F 66  |..Certificate of|
20 41 6E 64  72 65 79 20  46 65 64 6F  74 6F 76 03  | Andrey Fedotov.|
01 00 30 06  04 04 00 00  00 02 A1 82  05 0A A0 82  |..0.............|
03 BF 30 82  03 6E A0 03  02 01 02 02  0A 61 4A 76  |..0..n.......aJv|
22 00 00 00  00 00 1D 30  08 06 06 2A  85 03 02 02  |"......0...*....|
03 30 7A 31  23 30 21 06  09 2A 86 48  86 F7 0D 01  |.0z1#0!..*.H....|
09 01 16 14  6D 69 76 61  6E 6F 76 40  66 61 63 74  |....mivanov@fact|
6F 72 2D 74  73 2E 72 75  31 0B 30 09  06 03 55 04  |or-ts.ru1.0...U.|
06 13 02 52  55 31 0F 30  0D 06 03 55  04 07 13 06  |...RU1.0...U....|
4D 6F 73 63  6F 77 31 12  30 10 06 03  55 04 0A 13  |Moscow1.0...U...|
09 43 72 79  70 74 6F 50  72 6F 31 0E  30 0C 06 03  |.CryptoPro1.0...|
55 04 0B 13  05 50 72 6F  6D 6F 31 11  30 0F 06 03  |U....Promo1.0...|
55 04 03 13  08 4D 61 78  69 6D 20 55  43 30 1E 17  |U....Maxim UC0..|
0D 31 32 30  35 31 38 31  31 30 33 30  30 5A 17 0D  |.1205181103 00Z..|
31 33 30 35  31 38 31 31  31 32 30 30  5A 30 81 BA  |130518111200Z0..|
31 23 30 21  06 09 2A 86  48 86 F7 0D  01 09 01 16  |1#0!..*.H.......|
14 66 65 64  6F 74 6F 76  40 66 61 63  74 6F 72 2D  |.fedotov@factor-|
74 73 2E 72  75 31 0B 30  09 06 03 55  04 06 13 02  |ts.ru1.0...U....|
52 55 31 15  30 13 06 03  55 04 07 1E  0C 04 1C 04  |RU1.0...U.......|
3E 04 41 04  3A 04 32 04  30 31 1B 30  19 06 03 55  |>.A.:.2.01.0...U|
04 0A 1E 12  04 24 04 30  04 3A 04 42  04 3E 04 40  |.....$.0.:.B.>.@|
00 2D 04 22  04 21 31 11  30 0F 06 03  55 04 0B 1E  |.-."."!1.0...U...|
08 04 22 04  35 04 41 04  42 31 3F 30  3D 06 03 55  |.."5.A.B1?0=..U|
04 03 1E 36  04 24 04 35  04 34 04 3E  04 42 04 3E  |...6.$.5.4.>.B.>|
```

```
04 32 00 20  04 10 04 3D  04 34 04 40  04 35 04 39  |.2. ...=.4.@.5.9|
00 20 04 12  04 3B 04 30  04 34 04 38  04 3C 04 38  |. ...;.0.4.8.<.8|
04 40 04 3E  04 32 04 38  04 47 30 63  30 1C 06 06  |.@.>.2.8.G0c0...|
2A 85 03 02  02 13 30 12  06 07 2A 85  03 02 02 23  |*.....0...*....#|
01 06 07 2A  85 03 02 02  1E 01 03 43  00 04 40 ED  |...*.......C..@.|
92 03 66 00  10 11 B9 AC  32 68 28 56  76 95 D2 4B  |..f.....2h(Vv..K|
B1 1F 22 66  82 FC 53 CC  91 CA 6A 0A  14 30 67 27  |.."f..S...j..0g'|
6A 53 43 D1  E2 93 16 4B  21 00 12 89  47 C8 86 F9  |jSC....K!...G...|
21 44 95 51  08 A7 45 E6  17 85 73 75  9D 64 4E A3  |!D.Q..E...su.dN.|
82 01 91 30  82 01 8D 30  0E 06 03 55  1D 0F 01 01  |...0...0...U....|
FF 04 04 03  02 04 F0 30  13 06 03 55  1D 25 04 0C  |.......0...U.%..|
30 0A 06 08  2B 06 01 05  05 08 02 02  30 1D 06 03  |0...+.......0...|
55 1D 0E 04  16 04 14 52  58 AD 0C 45  43 0D E5 F6  |U......RX..EC...|
DE 39 7B 77  3B 3D F9 1D  69 FF 39 30  1F 06 03 55  |.9{w;=..i.90...U|
1D 23 04 18  30 16 80 14  C3 99 AC 2E  F8 F6 FC F0  |.#..0...........|
62 2C 8A 80  35 DF DA 63  28 17 EF ED  30 75 06 03  |b,..5..c(...0u..|
55 1D 1F 04  6E 30 6C 30  6A A0 68 A0  66 86 30 68  |U...n0l0j.h.f.0h|
74 74 70 3A  2F 2F 76 6F  65 6E 6D 65  68 2D 64 30  |ttp://voenmeh-d0|
66 32 38 36  61 2F 43 65  72 74 45 6E  72 6F 6C 6C  |f286a/CertEnroll|
2F 4D 61 78  69 6D 25 32  30 55 43 2E  63 72 6C 86  |/Maxim%20UC.crl.|
32 66 69 6C  65 3A 2F 2F  5C 5C 76 6F  65 6E 6D 65  |2file://\\voenme|
68 2D 64 30  66 32 38 36  61 5C 43 65  72 74 45 6E  |h-d0f286a\CertEn|
72 6F 6C 6C  5C 4D 61 78  69 6D 25 32  30 55 43 2E  |roll\Maxim%20UC.|
63 72 6C 30  81 AE 06 08  2B 06 01 05  05 07 01 01  |crl0....+.......|
04 81 A1 30  81 9E 30 4C  06 08 2B 06  01 05 05 07  |...0..0L..+.....|
30 02 86 40  68 74 74 70  3A 2F 2F 76  6F 65 6E 6D  |0..@http://voenm|
65 68 2D 64  30 66 32 38  36 61 2F 43  65 72 74 45  |eh-d0f286a/CertE|
6E 72 6F 6C  6C 2F 76 6F  65 6E 6D 65  68 2D 64 30  |nroll/voenmeh-d0|
66 32 38 36  61 5F 4D 61  78 69 6D 25  32 30 55 43  |f286a_Maxim%20UC|
2E 63 72 74  30 4E 06 08  2B 06 01 05  05 07 30 02  |.crt0N..+.....0.|
86 42 66 69  6C 65 3A 2F  2F 5C 5C 76  6F 65 6E 6D  |.Bfile://\\voenm|
65 68 2D 64  30 66 32 38  36 61 5C 43  65 72 74 45  |eh-d0f286a\CertE|
6E 72 6F 6C  6C 5C 76 6F  65 6E 6D 65  68 2D 64 30  |nroll\voenmeh-d0|
66 32 38 36  61 5F 4D 61  78 69 6D 25  32 30 55 43  |f286a_Maxim%20UC|
2E 63 72 74  30 08 06 06  2A 85 03 02  02 03 03 41  |.crt0...*......A|
00 71 DB 23  67 25 9C C9  D0 86 2A C9  1D D9 9D AA  |.q.#g%....*.....|
C8 51 BC A9  2C BA F4 82  F3 F4 8E CF  0C 81 77 A7  |.Q..,.........w.|
2F 35 34 8A  D8 9B B1 B0  0A 18 50 A2  7E CF 8A 6D  |/54.......P.~..m|
CB 5E 53 21  88 08 EC F3  CA 7A 36 02  8D A2 F1 F5  |.^S!.....z6.....|
E4 30 81 BA  31 23 30 21  06 09 2A 86  48 86 F7 0D  |.0..1#0!..*.H...|
01 09 01 16  14 66 65 64  6F 74 6F 76  40 66 61 63  |.....fedotov@fac|
74 6F 72 2D  74 73 2E 72  75 31 0B 30  09 06 03 55  |tor-ts.ru1.0...U|
04 06 13 02  52 55 31 15  30 13 06 03  55 04 07 1E  |....RU1.0...U...|
0C 04 1C 04  3E 04 41 04  3A 04 32 04  30 31 1B 30  |....>.A.:.2.01.0|
19 06 03 55  04 0A 1E 12  04 24 04 30  04 3A 04 42  |...U.....$.0.:.B|
04 3E 04 40  00 2D 04 22  04 21 31 11  30 0F 06 03  |.>.@.-.".!1.0...|
55 04 0B 1E  08 04 22 04  35 04 41 04  42 31 3F 30  |U.....".5.A.B1?0|
3D 06 03 55  04 03 1E 36  04 24 04 35  04 34 04 3E  |=..U...6.$.5.4.>|
04 42 04 3E  04 32 00 20  04 10 04 3D  04 34 04 40  |.B.>.2. ...=.4.@|
04 35 04 39  00 20 04 12  04 3B 04 30  04 34 04 38  |.5.9. ...;.0.4.8|
04 3C 04 38  04 40 04 3E  04 32 04 38  04 47 A0 7C  |.<.8.@.>.2.8.G.||
30 7A 31 23  30 21 06 09  2A 86 48 86  F7 0D 01 09  |0z1#0!..*.H.....|
01 16 14 6D  69 76 61 6E  6F 76 40 66  61 63 74 6F  |...mivanov@facto|
72 2D 74 73  2E 72 75 31  0B 30 09 06  03 55 04 06  |r-ts.ru1.0...U..|
13 02 52 55  31 0F 30 0D  06 03 55 04  07 13 06 4D  |..RU1.0...U....M|
6F 73 63 6F  77 31 12 30  10 06 03 55  04 0A 13 09  |oscow1.0...U....|
43 72 79 70  74 6F 50 72  6F 31 0E 30  0C 06 03 55  |CryptoPro1.0...U|
04 0B 13 05  50 72 6F 6D  6F 31 11 30  0F 06 03 55  |....Promo1.0...U|
04 03 13 08  4D 61 78 69  6D 20 55 43  02 0A 61 4A  |....Maxim UC..aJ|
76 22 00 00  00 00 00 1D  A0 82 01 40  A0 82 01 3C  |v".........@...<|
BA 82 01 38  30 1F 0C 19  4E 65 77 20  47 65 6E 65  |...80...New Gene|
72 61 74 65  64 20 50 72  69 76 61 74  65 20 4B 65  |rated Private Ke|
79 03 02 07  80 30 0E 04  04 00 00 00  03 03 02 05  |y....0..........|
20 03 02 05  E0 A1 82 01  03 A2 81 F5  02 01 02 31  | ..............1|
59 A2 57 02  01 04 30 06  04 04 00 00  00 04 30 1E  |Y.W...0.......0.|
06 07 2A 85  03 02 02 0D  01 30 13 06  07 2A 85 03  |..*......0...*..|
02 02 1F 01  04 08 26 30  47 72 9C E3  74 6F 04 2A  |......&0Gr..to.*|
30 28 04 20  D6 B9 95 95  DD 7A D6 C3  E6 7D FC 52  |0(. .....z...}.R|
19 6E C6 35  4E 3E 95 0B  DE 23 C1 23  CB 76 61 98  |.n.5N>...#.#.va.|
E4 2E 75 19  04 04 FD B5  BD 92 30 81  94 06 09 2A  |..u.......0....*|
86 48 86 F7  0D 01 07 01  30 1F 06 08  2A 85 03 02  |.H......0...*...|
04 03 02 02  30 13 04 08  64 59 E7 C7  14 DE 0A E3  |....0...dY......|
06 07 2A 85  03 02 02 1F  01 80 66 17  FA 51 6A 7E  |..*.......f..Qj~|
0C 59 F3 E8  72 F0 7B 8D  BE 3D F1 D6  76 CF D1 18  |.Y..r.{..=..v...|
C9 00 7D B1  90 77 E4 6F  68 10 27 D4  5D 11 A4 8E  |..}..w.oh.'.]...|
75 C1 20 DB  9C 73 A4 8A  93 3C EA 26  9E CF 3E 06  |u. ..s...<.&..>.|
41 E6 02 C4  0B B6 C9 CD  05 06 4E B5  2B 12 74 09  |A.........N.+.t.|
BE 45 4D E2  98 8C CF 66  FC 5F 57 07  3D B2 41 8B  |.EM....f._W.=.A.|
B9 B6 85 FE  0F D4 7F 7B  D2 E0 EF 32  2C 62 83 F4  |.......{...2,b..|
```

```
07 30 09 06  07 2A 85 03  02 02 23 02  A1 81 92 A0  |.0...*....#.....|
81 8F BA 81  8C 30 2D 0C  28 50 75 62  6C 69 63 20  |.....0-.(Public |
4B 65 79 20  66 6F 72 20  4E 65 77 20  47 65 6E 65  |Key for New Gene|
72 61 74 65  64 20 50 72  69 76 61 74  65 20 4B 65  |rated Private Ke|
79 03 01 00  30 0A 04 04  00 00 00 03  03 02 01 02  |y...0...........|
A1 4F A0 42  04 40 1E 8B  CE FD 7C 95  E8 4F 11 E3  |.O.B.@....|..O..|
5A 14 A0 58  FD 5B CB 3E  24 89 3A DE  91 59 99 EB  |Z..X.[.>$.:..Y..|
27 5B A3 AF  AF 1D D4 D5  8D 6C 32 A2  64 D3 8A E6  |'[.......l2.d...|
CD 07 54 0C  76 7B 41 5E  64 54 0B E9  23 02 A7 F4  |..T.v{A^dT..#...|
EA FA 65 CD  F6 4B 30 09  06 07 2A 85  03 02 02 23  |..e..K0...*....#|
02 A7 82 01  20 A0 82 01  1C A1 82 01  18 30 15 0C  |.... ........0..|
0F 54 6F 70  2D 73 65 63  72 65 74 20  44 61 74 61  |.Top-secret Data|
03 02 06 C0  30 0D 06 0B  2B 06 01 04  01 E8 00 83  |....0...+.......|
77 01 04 A1  81 EF 06 05  29 83 48 BD  52 A2 81 E5  |w.......).H.R...|
02 01 02 31  59 A2 57 02  01 04 30 06  04 04 00 00  |...1Y.W...0.....|
00 04 30 1E  06 07 2A 85  03 02 02 0D  01 30 13 06  |..0...*......0..|
07 2A 85 03  02 02 1F 01  04 08 72 1F  F5 35 95 22  |.*........r..5."|
EC C2 04 2A  30 28 04 20  F2 D2 EE E6  12 44 64 20  |...*0(. .....Dd |
97 1F 02 A7  D2 0C C5 D5  77 46 96 F0  3D F8 B5 62  |........wF..=..b|
3D A9 45 0A  E6 DF 6D 64  04 04 E2 0A  7F 02 30 81  |=.E...md......0.|
84 06 09 2A  86 48 86 F7  0D 01 07 01  30 1F 06 08  |...*.H......0...|
2A 85 03 02  04 03 02 02  30 13 04 08  3F 90 96 7B  |*.......0...?..{|
F8 3F 30 1D  06 07 2A 85  03 02 02 1F  01 80 56 15  |.?0...*.......V.|
9D C1 8F 62  07 70 D0 03  31 74 DF A7  02 5C D9 22  |...b.p..1t...\."|
3C F2 97 AA  D5 D4 F1 C5  E7 06 04 64  F9 73 2E 64  |<..........d.s.d|
B4 5B C2 50  4A 52 64 B0  A9 FB 07 27  F5 37 58 EF  |.[.PJRd....'.7X.|
4D B0 BD A3  69 A1 A8 77  2C 15 25 8E  50 07 8F E0  |M...i..w,.%.P...|
CA 14 EF F6  3A C1 16 19  76 C9 31 DB  A3 37 6D 96  |....:...v.1..7m.|
F6 8C 81 6B  68 A7 6B A0  69 A1 67 30  11 0C 0B 50  |...kh.k.i.g0...P|
75 62 6C 69  63 20 44 61  74 61 03 02  06 40 30 0D  |ublic Data...@0.|
06 0B 2B 06  01 04 01 E8  00 83 77 01  04 A1 43 06  |..+.......w...C.|
06 29 85 7D  83 30 01 A0  39 04 37 54  68 69 73 20  |.).}.0..9.7This |
69 73 20 73  6F 6D 65 20  6F 70 65 6E  20 64 61 74  |is some open dat|
61 2E 20 54  68 65 72 65  27 73 20 6E  6F 20 6E 65  |a. There's no ne|
65 64 20 74  6F 20 65 6E  63 72 79 70  74 20 69 74  |ed to encrypt it|
2E 00                                              |..              |
Message digest (hash) of the eContent (ostr header not included):
64 4E D1 DA  ED D7 ED BB  0A D8 1C 4E  A8 03 4E 41  |dN.........N..NA|
F9 04 A7 D0  02 15 23 3A  83 9C 7E EE  B0 BE 74 68  |......#:..~...th|

Making AuthenticatedData.authAttrs:
attr1 (id-contentType):
attr1.attrType: 1.2.840.113549.1.9.3
attr1.attrValue1: 1.2.840.113549.1.15.3.1
attr2 (id-messageDigest):
attr2.attrType: 1.2.840.113549.1.9.4
attr2.attrValue1: ostr len=32 - message digest (see above)

Encoded authAttrs (standalone):
31 4C 30 19  06 09 2A 86  48 86 F7 0D  01 09 03 31  |1L0...*.H......1|
0C 06 0A 2A  86 48 86 F7  0D 01 0F 03  01 30 2F 06  |...*.H.......0/.|
09 2A 86 48  86 F7 0D 01  09 04 31 22  04 20 64 4E  |.*.H......1". dN|
D1 DA ED D7  ED BB 0A D8  1C 4E A8 03  4E 41 F9 04  |.........N..NA..|
A7 D0 02 15  23 3A 83 9C  7E EE B0 BE  74 68        |....#:..~...th  |
Calculating HMAC of authAttr:
Key:
D9 89 7F 8D  E7 98 F6 9A  45 85 8B 89  76 62 50 7C  |........E...vbP||
C5 63 3F A4  F5 0C F5 A0  49 68 9B 63  1F F3 61 09  |.c?.....Ih.c..a.|
authAttrs HMAC (AuthenticatedData.mac):
FA FD 4D 0E  63 7F 29 11  59 1D 5D 3F  AF A6 0C C4  |..M.c.).Y.]?....|
E7 F1 36 2E  93 59 E2 5C  D5 68 E5 B0  FA 5B 15 39  |..6..Y.\.h...[.9|
```

## Литература


1. PKCS #15 v1.1: Cryptographic Token Information Syntax Standard
2. RFC5652: Cryptographic Message Syntax
3. RFC4357: Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001, and GOST R 34.11–94 Algorithms
4. RFC4491: Using the GOST R 34.10–94, GOST R 34.10–2001, and GOST R 34.11–94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
5. RFC4490: Using the GOST 28147–89, GOST R 34.11–94, GOST R 34.10–94, and GOST R 34.10–2001 Algorithms with Cryptographic Message Syntax (CMS)
6. Парольная защита с использованием алгоритмов ГОСТ. Дополнения к PKCS#5 (версия 1.0)
7. Транспортный ключевой контейнер. Дополнения к PKCS#8 и PKCS#12 (версия 1.0)