ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

Р 50.1.110—2016

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Контейнер хранения ключей

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ подкомитетом 2 Технического комитета по стандартизации ТК 26 «Криптографическая защита информации»

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 23 ноября 2016 г. № 1751-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и обозначения 1
4 Базовые типы [1] 2
5 Объекты для хранения ключей 2
5.1 Представление ключа 2
5.2 Объект закрытого ключа 3
5.3 Объект открытого ключа 3
5.4 Объект симметричного ключа 4
6 Обеспечение конфиденциальности ключей 5
7 Обеспечение целостности информации 6
8 Общая структура контейнера хранения ключей 7
Приложение А (справочное) ASN.1 модуль контейнера хранения ключей 8
Приложение Б (справочное) Контрольный пример 14
Библиография 39

Введение

Настоящие рекомендации содержат описание расширения документа PKCS#15 «Cryptographic Token Information Format Standard» [1], разработанного и опубликованного RSA Laboratories. Он описывает синтаксис представления ключевой информации, цифровых сертификатов, аутентификационной информации и других данных при их хранении на внешних носителях.

Данное расширение [1] позволяет использовать синтаксис базового стандарта для создания контейнеров хранения ключевой информации, используемой в криптографических алгоритмах по ГОСТ Р 34.10 и ГОСТ 28147—89.

Целесообразность разработки настоящих рекомендаций вызвана потребностью в унифицированном решении, использующем национальные криптографические стандарты и позволяющем обеспечить совместимость средств криптографической защиты различных разработчиков в части формата хранения ключевой информации на носителе пользователя.

Примечание — Основная часть настоящих рекомендаций дополнена приложениями А и Б.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Контейнер хранения ключей

Information technology. Cryptographic data security.
Key storage container

Дата введения — 2017—06—01

1 Область применения

Настоящие рекомендации предназначены для применения в общедоступных информационно-телекоммуникационных, корпоративных сетях и информационных системах для защиты информации, не содержащей сведений, составляющих государственную тайну, с использованием механизмов шифрования и защиты аутентичности данных.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 34.10 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ 28147—89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

Р 50.1.111—2016 Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации

Р 50.1.112—2016 Информационная технология. Криптографическая защита информации. Транспортный ключевой контейнер

Р 50.1.113—2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов (рекомендаций) в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт (рекомендации), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (рекомендаций) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (рекомендации), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (рекомендаций) с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт (рекомендации), на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт (рекомендации) отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

В настоящих рекомендациях применены термины, определения и обозначения, определенные в документах, приведенных в разделе «Библиография».

Издание официальное

4 Базовые типы [1]

Базовые типы подробно описаны в 6.1 [1]. Этих базовых типов достаточно для спецификации информации о ключах, включая назначение ключей, сроки действия, данные о владельце, издателе и т. п.

В [1] отсутствует определение «имя контейнера», и для наименования объектов применена метка (6.1.3 [1]).

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

Объекты закрытых, открытых ключей и сертификатов содержат идентификатор iD (см. структуры CommonKeyAttributes, CommonCertificateAttributes [1]). Идентификатор имеет следующий тип:

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

Идентификатор является уникальным для объекта одного типа в рамках одного контейнера [1]. Совпадение идентификаторов объектов разного типа означает их взаимосвязь. Например, соответствие закрытого ключа открытому ключу или соответствие ключа сертификату.

Для идентификации ключей также могут использоваться поля subjectName, содержащие имя субъекта ключа (см. структуры CommonPrivateKeyAttributes, CommonPublicKeyAttributes [1]).

В [1] объекты могут храниться как в виде значений, так и в виде ссылок на другие объекты. Для этого применен тип данных PathOrObjects (6.1.7 [1]).

```
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},
}
```

Настоящие рекомендации определяют, что для хранения неконфиденциальных объектов (открытые ключи, сертификаты) должен использоваться вариант objects[0], а для хранения конфиденциальных объектов (закрытые и симметричные ключи) — вариант direct-protected[2].

Для идентификации параметров объектов и области их применения используется тип KeyInfo (6.1.13 [1]).

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

Сами объекты [1] представляют собой набор атрибутов разного уровня детализации, позволяющих описать 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
}
```

5 Объекты для хранения ключей

[1] определено, что в контейнере могут храниться ключи трех типов: закрытые, открытые и симметричные. Ниже определены расширения соответствующих структур для хранения ключей алгоритмов ГОСТ Р 34.10 и ГОСТ 28147—89.

5.1 Представление ключа

Для обеспечения защиты закрытых и симметричных ключей от утечек по побочным каналам при считывании и проведении операций с ключами целесообразно использование маскированных

ключей. Для хранения маскированных ключей и наборов масок использованы представления ключей в виде:

GostR3410-2012-KeyValueMask ::= OCTET STRING { $K_m|M_1|M_2|....|M_k$ }

Gost28147-89-KeyValueMask ::= OCTET STRING { $K_m|M_1|M_2|....|M_k$ }

Подробное описание данных представлений ключей изложено в разделе 4 Р 50.1.112—2016.

5.2 Объект закрытого ключа

В соответствии с 6.3.1 [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, выработанных по алгоритму ГОСТ Р 34.10, в структуру PrivateKeyType введен следующий тип ключа:

```
privateGostR3410-2012Key [27] PrivateKeyObject {
        PrivateGostR3410-2012KeyAttributes}

PrivateGostR3410-2012KeyAttributes ::= SEQUENCE {
        value ObjectValue {GostR3410-2012PrivateKey},
        keyInfo KeyInfo {GostPrivateKeyParameters, PublicKeyOperations}
                OPTIONAL,
        ... -- For future extensions
}

GostR3410-2012PrivateKey ::= GostR3410-2012-KeyValueMask

GostPrivateKeyParameters ::= CHOICE {
        gostR3410-2012ParamSet OBJECT IDENTIFIER,
        privateKeyParamSet [0] GostR3410-2001-ParamSetParameters,
        ...
}
,
```

где gostR3410-2012ParamSet — идентификатор параметров алгоритма, который выбран в соответствии с «Идентификаторы объектов (OID) технического комитета по стандартизации» [2]. Рекомендуется использовать значение id-tc26-gost-3410-12-512-paramSetA.

Если структура keyInfo отсутствует, то предполагается значение параметров по умолчанию:

KeyInfo.paramsAndOps.parameters = id-tc26-gost-3410-12-512-paramSetA

5.3 Объект открытого ключа

В 6.4.1 [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, выработанного по алгоритму ГОСТ Р 34.10, в структуру PublicKeyType введен следующий тип:

```
publicGostR3410-2012Key [27] PublicKeyObject {
        PublicGostR3410-2012KeyAttributes}

PublicGostR3410-2012KeyAttributes ::= SEQUENCE {
        value ObjectValue {GostR3410-2012PublicKeyChoice},
        keyInfo KeyInfo {GostPrivateKeyParameters, PublicKeyOperations}
                OPTIONAL,
        ... -- For future extensions
}

GostR3410-2012PublicKeyChoice ::= CHOICE {
        raw GostR3410-2012Point,
        spki SubjectPublicKeyInfo,
        ...
}
```

При использовании SubjectPublicKeyInfo открытый ключ и его параметры должны быть представлены в соответствии с 4.3 [3]. Поле SubjectPublicKeyInfo.algorithm.parameters не должно быть NULL.

При использовании GostR3410-2012Point открытый ключ должен иметь представление, описанное в Р 50.1.112 — 2016.

GostR3410-2012Point ::= GostR3410-2012-PublicKey.

Если структура keyInfo отсутствует, то предполагается значение параметров по умолчанию:

KeyInfo.paramsAndOps.parameters = id-tc26-gost-3410-12-512-paramSetA

5.4 Объект симметричного ключа

Структура симметричного секретного ключа определена в 6.5.1 [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}
```

Для хранения симметричного ключа для алгоритма ГОСТ 28147—89 в структуру SecretKeyType введен тип:

```
gostKey [27] GostSecretKey
```

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

В качестве идентификатора типа ключа должен быть представлен идентификатор алгоритма в соответствии с 8.1 [4]:

keyTypeGost = id-Gost28147-89

Атрибуты симметричного ключа определены следующим образом:

```
GostSecretKeyAttributes ::= SEQUENCE {
        value ObjectValue {Gost28147-89-KeyValueMask},
        keyInfo KeyInfo {GostSecretKeyParameters, SecretKeyOperations}
                OPTIONAL,
        ...
}

GostSecretKeyParameters ::= CHOICE {
        cryptoProParamSet OBJECT IDENTIFIER,
        secretKeyParamSet [0] Gost28147-89-ParamSetParameters,
        ...
}
SecretKeyOperations ::= Operations
```

Идентификаторы параметров алгоритма cryptoProParamSet выбираются в соответствии с 8.1 RFC4357 [4] и разделом 4 [5].

Структура Gost28147-89-ParamSetParameters определена в 8.1 [4].

Если структура keyInfo отсутствует, то принимается значение по умолчанию:

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

6 Обеспечение конфиденциальности ключей

Для обеспечения конфиденциальности объектов закрытого и симметричного ключа в соответствии с [1] использован тип EnvelopedData. Данный тип определен в разделе 6 [6].

```
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 представлено 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 инкапсулированных данных Type в соответствии с 7.3 [1] идентифицирован как:

```
pkcs15-ct-PKCS15Token OBJECT IDENTIFIER ::= {pkcs15-ct 1}
pkcs15-ct OBJECT IDENTIFIER ::= {pkcs15 3}
pkcs15 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
        rsadsi(113549) pkcs(1) pkcs-15(15)}
```

При шифровании должен быть использован алгоритм ГОСТ 28147—89. Алгоритм и параметры шифрования contentEncryptionAlgorithm указывают в соответствии с 5.1 [7] и разделом 5 [5].

Могут быть использованы алгоритмы шифрования с завершающей имитовставкой:
Алгоритм гаммирования с обратной связью (раздел 4 ГОСТ 28147—89):

```
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 (раздел 3 ГОСТ 28147—89):

```
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 указаны в соответствии с 5.1. [7] и раздел 5 [5]. Зашифрованные данные содержат результат зашифрования конкатенированный с имитовставкой, вычисленной на тех же параметрах, что и при зашифровании.

В качестве ключа шифрования (Key Encryption Key, KEK) использован симметричный ключ ГОСТ 28147—89. Информация о ключе шифрования размещена 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 (6.2.3 и 6.2.4 [6] 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 в соответствии с 7.1 Р 50.1.111—2016.

При шифровании ключа должен быть использован алгоритм ГОСТ 28147—89. Алгоритм и параметры шифрования keyEncryptionAlgorithm указаны в соответствии с 5.1 [7] и разделом 5 [5].

Зашифрованный ключ представлен в виде:

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

7 Обеспечение целостности информации

Для обеспечения целостности ключей результирующая структура PKCS15Token инкапсулирована в AuthenticatedData в соответствии с 9 [6] и E.1.3 [1] с использованием алгоритма HMAC_GOSTR3411_2012_512 по Р 50.1.113—2016.

```
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
}
MessageAuthenticationCodeAlgorithm  ::= AlgorithmIdentifier
```

Использован следующий идентификатор алгоритма:

```
MessageAuthenticationCodeAlgorithm.algorithm
        = id-tc26-hmac-gost-3411-12-512
```

Параметры HMAC_GOSTR3411_2012_512 не указаны:

```
MessageAuthenticationCodeAlgorithm. parameters = NULL
```

8 Общая структура контейнера хранения ключей

В соответствии с 7.3 и E [1] контейнер хранения ключей может быть представлен в структурах трех видов:

1) структура PKCS15Token в соответствии с [1];
2) структура AuthenticatedData в соответствии с [6], инкапсулирующая структуру PKCS15Token;
3) структура SignedData в соответствии с [6] и [8], инкапсулирующая структуру PKCS15Token.

Структуры видов 2 и 3 используют в тех случаях, когда необходимо обеспечить целостность контейнера хранения ключей.

В соответствии с 7.3 [1] структура PKCS15Token определена, как:

```
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--})
```

При использовании представления информации в виде pwri в KeyManagementInfo фактически дублируется информация о шифровании ключа в структуре EnvelopedData. Данную информацию можно опционально использовать для выбора и предварительной проверки пароля в том случае, если для разных объектов используют 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.

Приложение А
(справочное)

ASN.1 модуль контейнера хранения ключей

```
PKCS15-GOST-v2-0
DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

AuthenticatedData, SignedData
    FROM CryptographicMessageSyntax2004 { iso(1) member-body(2) us(840)
    rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }

PKCS15Token, PrivateKeyObject, PublicKeyOperations, PublicKeyObject, ObjectValue,
Operations, SecretKeyObject, SubjectPublicKeyInfo, KeyInfo
    FROM PKCS-15 {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-15(15)
        modules(1) pkcs-15(1)}

ALGORITHM-IDENTIFIER, id-PBKDF2, PBKDF2-params
    FROM PKCS5v2-0 {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-5(5)
    modules(16) pkcs5v2-0(1)}

GostR3410-2001-ParamSetParameters
    FROM GostR3410-2001-ParamSetSyntax { iso(1) member-body(2) ru(643) rans(2)
        cryptopro(2) other(1) modules(1) gostR3410-2001-ParamSetSyntax(12) 1 }

id-GostR3410-2001-TestParamSet, id-GostR3410-2001-CryptoPro-A-ParamSet,
id-GostR3410-2001-CryptoPro-B-ParamSet, id-GostR3410-2001-CryptoPro-C-ParamSet,
id-GostR3410-2001-CryptoPro-XchA-ParamSet, id-GostR3410-2001-CryptoPro-XchB-ParamSet
    FROM GostR3410-2001-PKISyntax { iso(1) member-body(2) ru(643) rans(2)
        cryptopro(2) other(1) modules(1) gostR3410-2001-PKISyntax(9) 1 }

id-Gost28147-89-CryptoPro-KeyWrap
    FROM GostR3410-EncryptionSyntax { iso(1) member-body(2) ru(643) rans(2)
        cryptopro(2) other(1) modules(1) gostR3410-EncryptionSyntax(5) 2 }

id-Gost28147-89, id-Gost28147-89-TestParamSet, id-Gost28147-89-CryptoPro-A-ParamSet,
id-Gost28147-89-CryptoPro-B-ParamSet, id-Gost28147-89-CryptoPro-C-ParamSet,
id-Gost28147-89-CryptoPro-D-ParamSet, id-Gost28147-89-CryptoPro-Oscar-1-1-ParamSet,
id-Gost28147-89-CryptoPro-Oscar-1-0-ParamSet,id-Gost28147-89-CryptoPro-RIC-1-ParamSet,
Gost28147-89-IV
    FROM Gost28147-89-EncryptionSyntax { iso(1) member-body(2) ru(643) rans(2)
        cryptopro(2) other(1) modules(1) gost28147-89-EncryptionSyntax(4) 1 }

Gost28147-89-ParamSetParameters
    FROM Gost28147-89-ParamSetSyntax { iso(1) member-body(2) ru(643) rans(2)
        cryptopro(2) other(1) modules(1) gost28147-89-ParamSetSyntax(6) 1 }

;


-- OID-ы

id-tc26  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) ru(643) std-org(7) tc26(1) }
```

```
id-tc26-algorithms OBJECT IDENTIFIER ::=
    { id-tc26 algorithms(1) }

id-tc26-digest OBJECT IDENTIFIER ::=
    { id-tc26-algorithms digest(2) }

id-tc26-gost3411-12-512 OBJECT IDENTIFIER ::=
    { id-tc26-digest gost3411-12-512(3) }

id-tc26-mac OBJECT IDENTIFIER ::=
    { id-tc26-algorithms mac(4) }

id-tc26-hmac-gost3411-12-512 OBJECT IDENTIFIER ::=
    { id-tc26-mac hmac-gost3411-12-512(2) }

id-tc26-constants OBJECT IDENTIFIER ::=
    { id-tc26 constants(2) }

id-tc26-sign-constants OBJECT IDENTIFIER ::=
    { id-tc26-constants sign-constants(1) }

id-tc26-gost3410-12-512-constants OBJECT IDENTIFIER ::=
    { id-tc26-sign-constants gost3410-12-512-constants(2) }

id-tc26-gost3410-12-512-paramSetTest OBJECT IDENTIFIER ::=
    { id-tc26-gost3410-12-512-constants paramSetTest(0) }

id-tc26-gost3410-12-512-paramSetA OBJECT IDENTIFIER ::=
    { id-tc26-gost3410-12-512-constants paramSetA(1) }

id-tc26-gost3410-12-512-paramSetB OBJECT IDENTIFIER ::=
    { id-tc26-gost3410-12-512-constants paramSetB(2) }

id-tc26-cipher-constants OBJECT IDENTIFIER ::=
    { id-tc26-constants cipher-constants(5) }

id-tc26-gost-28147-constants OBJECT IDENTIFIER ::=
    { id-tc26-cipher-constants gost-28147-constants(1) }

id-tc26-gost-28147-param-Z OBJECT IDENTIFIER ::=
    { id-tc26-gost-28147-constants param-Z(1) }

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

id-Gost28147-89-cbc-imm OBJECT IDENTIFIER ::=
        { id-infotecs-gost28147-algorithms cbc-imm(2) }

id-Gost28147-89-cnt-imm OBJECT IDENTIFIER ::=
        { id-infotecs-gost28147-algorithms cnt-imm(3) }

-- Контейнеры PKCS15-GOST

PKCS15-GOST-Token ::= PKCS15Token (CONSTRAINED BY {
-- 1. Разделы 7.2, 7.3 и E.1.2 в "PKCS #15 v1.1: Cryptographic Token Information
--    Format Standard".
-- 2. В структуре 'PathOrObjects' должны использоваться варианты 'objects' или
-- 'direct-protected' (для открытых и зашифрованных объектов соответственно).
-- 3. Все ссылки на 'ContentEncryptionAlgorithms' должны быть заменены на
--    'ContentEncryptionAlgorithmsGost'.
```

```
-- 4. Все ссылки на 'KeyDerivationAlgorithms' должны быть заменены на
--    'KeyDerivationAlgorithmsGost'.
-- 5. Все ссылки на 'KeyEncryptionAlgorithms' должны быть заменены на
--    'KeyEncryptionAlgorithmsGost'.
-- 6. В структурах 'RecipientInfo' должны использоваться только варианты 'kekri'
--    и 'pwri'.
-- 7. Все ссылки на 'PrivateKeyType' должны быть заменены на 'PrivateKeyTypeGost'.
-- 8. Все ссылки на 'PublicKeyType' должны быть заменены на 'PublicKeyTypeGost'.
-- 9. Все ссылки на 'SecretKeyType' должны быть заменены на 'SecretKeyTypeGost'.
})

PKCS15-GOST-AuthenticatedToken ::= AuthenticatedData (CONSTRAINED BY {
-- 1. Разделы 7.3 и E.1.3 в "PKCS #15 v1.1: Cryptographic Token Information
--    Format Standard".
-- 2. Все ссылки на 'PKCS15Token' должны быть заменены на 'PKCS15-GOST-Token'.
-- 3. Все ссылки на 'KeyEncryptionAlgorithms' должны быть заменены на
--    'KeyEncryptionAlgorithmsGost'.
-- 4. Все ссылки на 'DigestAlgorithms' должны быть заменены на 'DigestAlgorithmsGost'.
-- 5. Все ссылки на 'MACAlgorithms' должны быть заменены на 'MACAlgorithmsGost'.
})

PKCS15-GOST-SignedToken ::= SignedData (CONSTRAINED BY {
-- 1. Раздел 7.3 в "PKCS #15 v1.1: Cryptographic Token Information Format Standard".
-- 2. "Методические рекомендации ТК 26. Использование алгоритмов ГОСТ 28147-89,
--    ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS".
-- 3. Все ссылки на 'PKCS15Token' должны быть заменены на 'PKCS15-GOST-Token'.
})

-- Типы для PKCS15-GOST

-- OID-ы и наборы параметров

GostSecretKeyAlgs OBJECT IDENTIFIER ::= {
    id-Gost28147-89,
    ...
}

Gost28147-89-ParamSets OBJECT IDENTIFIER ::= {
    Gost28147-89-CryptoPro-ParamSets |
    Gost28147-89-TC26-ParamSets
}

Gost28147-89-CryptoPro-ParamSets OBJECT IDENTIFIER ::= {
    id-Gost28147-89-TestParamSet |  -- Only for testing purposes
    id-Gost28147-89-CryptoPro-A-ParamSet |
    id-Gost28147-89-CryptoPro-B-ParamSet |
    id-Gost28147-89-CryptoPro-C-ParamSet |
    id-Gost28147-89-CryptoPro-D-ParamSet |
    id-Gost28147-89-CryptoPro-Oscar-1-1-ParamSet |
    id-Gost28147-89-CryptoPro-Oscar-1-0-ParamSet |
    id-Gost28147-89-CryptoPro-RIC-1-ParamSet
}

Gost28147-89-TC26-ParamSets OBJECT IDENTIFIER ::= {
    id-tc26-gost-28147-param-Z,
    ...
}

Gost3410-2001-ParamSets OBJECT IDENTIFIER ::= {
    id-GostR3410-2001-TestParamSet | -- Only for testing purposes
    id-GostR3410-2001-CryptoPro-A-ParamSet |
    id-GostR3410-2001-CryptoPro-B-ParamSet |
    id-GostR3410-2001-CryptoPro-C-ParamSet |
```

```
    id-GostR3410-2001-CryptoPro-XchA-ParamSet |
    id-GostR3410-2001-CryptoPro-XchB-ParamSet,
    ...
}

Gost3410-2012-ParamSets OBJECT IDENTIFIER ::= {
    id-tc26-gost3410-12-512-paramSetTest | -- Only for testing purposes
    id-tc26-gost3410-12-512-paramSetA |
    id-tc26-gost3410-12-512-paramSetB,
    ...
}

ContentEncryptionAlgorithmsGost ALGORITHM-IDENTIFIER ::= {
    { Gost28147-89-Parameters IDENTIFIED BY id-Gost28147-89 } |
    { Gost28147-89-Parameters IDENTIFIED BY id-Gost28147-89-cbc-imm } |
    { Gost28147-89-Parameters IDENTIFIED BY id-Gost28147-89-cnt-imm },
    ...
}

KeyDerivationAlgorithmsGost ALGORITHM-IDENTIFIER ::= {
    { PBKDF2-Gost3411-2012-512-params IDENTIFIED BY id-PBKDF2 },
    ...
}

KeyEncryptionAlgorithmsGost ALGORITHM-IDENTIFIER ::= {
    { Gost28147-89-KeyWrapParameters IDENTIFIED BY id-Gost28147-89-CryptoPro-
    KeyWrap },
    ...
}

DigestAlgorithmsGost ALGORITHM-IDENTIFIER ::= {
    { NULL IDENTIFIED BY id-tc26-gost3411-12-512 },
    ...
}

MacAlgorithmsGost ALGORITHM-IDENTIFIER ::= {
    { NULL IDENTIFIED BY id-tc26-hmac-gost3411-12-512 },
    ...
}

Gost28147-89-Parameters ::= SEQUENCE {
    iv                  Gost28147-89-IV,
    encryptionParamSet  OBJECT IDENTIFIER (Gost28147-89-ParamSets)
}

PBKDF2-Gost3411-2012-512-params ::= PBKDF2-params (CONSTRAINED BY {
-- Рекомендации по стандартизации Р 50.1.111-2016   " Информационная технология.
-- Криптографическая защита информации. Парольная защита ключевой информации"
})

Gost28147-89-KeyWrapParameters ::= SEQUENCE {
    encryptionParamSet  OBJECT IDENTIFIER (Gost28147-89-ParamSets),
    ukm                 OCTET STRING (SIZE (8)) OPTIONAL
}

-- Закрытый ключ

PrivateKeyTypeGost ::= CHOICE {
    privateGostR3410-2012Key
              [27] PrivateKeyObject {PrivateGostR3410-2012KeyAttributes},
    ...
}
```

```
PrivateGostR3410-2012KeyAttributes ::= SEQUENCE {
    value ObjectValue {GostR3410-2012PrivateKey},
    keyInfo KeyInfo {GostPrivateKeyParameters, PublicKeyOperations} OPTIONAL,
    ...
}

GostR3410-2012PrivateKey ::= GostR3410-2012-KeyValueMask

GostR3410-2012-KeyValueMask ::= OCTET STRING (CONSTRAINED BY {
-- Рекомендации по стандартизации Р 50.1.112-2016   " Информационная технология.
--  Криптографическая защита информации. Транспортный ключевой контейнер"
})

GostPrivateKeyParameters ::= CHOICE {
    gostR3410-2012ParamSet   OBJECT IDENTIFIER
              (Gost3410-2001-ParamSets | Gost3410-2012-ParamSets),
    privateKeyParamSet   [0] GostR3410-2001-ParamSetParameters,
    ...
}

-- Открытый ключ

PublicKeyTypeGost ::= CHOICE {
    publicGostR3410-2012Key
                  [27] PublicKeyObject {PublicGostR3410-2012KeyAttributes},
    ...
}

PublicGostR3410-2012KeyAttributes ::= SEQUENCE {
    value ObjectValue {GostR3410-2012PublicKeyChoice},
    keyInfo KeyInfo {GostPrivateKeyParameters, PublicKeyOperations} OPTIONAL,
    ... -- For future extensions
}

GostR3410-2012PublicKeyChoice ::= CHOICE {
    raw GostR3410-2012Point,
    spki SubjectPublicKeyInfoGost,
...
}

GostR3410-2012Point ::= GostR3410-2012-PublicKey

GostR3410-2012-PublicKey ::= OCTET STRING (CONSTRAINED BY {
-- Рекомендации по стандартизации Р 50.1.112-2016   " Информационная технология.
--  Криптографическая защита информации. Транспортный ключевой контейнер"
})

SubjectPublicKeyInfoGost ::= SubjectPublicKeyInfo (CONSTRAINED BY {
-- Методические рекомендации ТК 26 "Техническая спецификация использования алго-
ритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертифи-
катов
-- (CRL) инфраструктуры открытых ключей X.509" (проект)
})

-- Secret Keys

SecretKeyTypeGost ::= CHOICE {
    gostKey              [27] GostSecretKey,
    ...
}
```

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

GostSecretKeyAttributes ::= SEQUENCE {
    value ObjectValue {Gost28147-89-KeyValueMask},
    keyInfo KeyInfo {GostSecretKeyParameters, SecretKeyOperations} OPTIONAL,
    ...
}

Gost28147-89-KeyValueMask ::= OCTET STRING (CONSTRAINED BY {
-- Рекомендации по стандартизации Р 50.1.112-2016   " Информационная технология.
--  Криптографическая защита информации. Транспортный ключевой контейнер"
})

GostSecretKeyParameters ::= CHOICE {
    cryptoProParamSet OBJECT IDENTIFIER (Gost28147-89-ParamSets),
    secretKeyParamSet [0] Gost28147-89-ParamSetParameters,
    ...
}

SecretKeyOperations ::= Operations

END
```

Приложение Б
(справочное)

Контрольный пример

В данном примере приведено значение контейнера хранения ключей, содержащего:
- начальное заполнение ДСЧ;
- корневой сертификат;
- список отзыва;
- сертификат пользователя 1;
- 256-разрядный закрытый ключ пользователя 1;
- 256-разрядный закрытый ключ пользователя 2;
- открытый ключ пользователя 2;
- 512-разрядный закрытый ключ пользователя 3;
- открытый ключ пользователя 3;
- секретные произвольные данные;
- открытые произвольные данные.

Для защиты секретных данных и обеспечения целостности контейнера использован пароль «123» (шестнадцатеричное представление — 31 32 33).

Значение контейнера хранения ключей (инкапсулированного в AuthenticatedData) в Base64 представлении:

MIIYHQIBADFZolcCAQQwBgQEAAAABTAeBgcqhQMCAg0BMBMGByqFAwICHwEECMkmMz2Uq2nEBCow
KAQg1F48CCMbv0pq9T9/Y/Qed0XWTlFjVuMwUvv50MLVSOsEBLT5OT8wCgYIKoUDBwEBBAKhCgYI
KoUDBwEBAgMwghbzBgoqhkiG9w0BDwMBoIIW4wSCFt8wghbbAgEAoE4wTAQEAAAABaBEMEIGCSqG
SIb3DQEFDDA1BCB0uu6gvst3Xk7JurUuAUqg7t/wloAUU2qO9BvLdvTT4wICB9ACASAwCgYIKoUD
BwEBBAIwghaEp4IBbaCCAWmhQDAWDBFGYWN0b3ItVFMgdmVyc2lvbgMBADANBgsrBgEEAegAg3cB
A6EXBgsrBgEEAegAg3cBA6AIMAYCAQSAAQChggEjMBcMEVJhbmRvbSBJbml0IFZhbHVlAwIGwDAN
BgsrBgEEAegAg3cBAaGB+AYLKwYBBAHoAIN3AQGigegCAQIxWaJXAgEEMAYEBAAAAAUwHgYHKoUD
AgINATATBgcqhQMCAh8BBAjwhgCKtBda9wQqMCgEIPNz0k0I3XVpi3jbijB8kPB94kTd7qyIgZtg
kh20VUyMBARLZi5YMIGHBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIwEwQI16qxLDK9rIAGByqFAwIC
HwGAWV7DW7JkvqEJHYwB2C+3ek2Jqg0Ak3Q4gizLLvHh1X6wISXbAW4WAHCF2xV7aV0ukVCrmqZg
7pVrX8/l5Gzvc8li30W5ridI3w3TkperiLtxyxFDoFxYGujhpYID/aCCA/kwggP1MBsMFlJvb3Qg
Q2VydGlmaWNhdGUgb2YgQ0EDAQAwCQQEAAAAAQEB/6GCA8mgggK5MIICaKADAgECAhAHSLrFkOrF
m0xPD+cEmJyoMAgGBiqFAwICAzB6MSMwIQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5y
dTELMAkGA1UEBhMCUlUxDzANBgNVBAcTBk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYD
VQQLEwVQcm9tbzERMA8GA1UEAxMITWF4aW0gVUMwHhcNMTIwMzIxMTIzOTM4WhcNMTcwMzIxMTI0
NjEyWjB6MSMwIQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUx
DzANBgNVBAcTBk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQcm9tbzERMA8G
A1UEAxMITWF4aW0gVUMwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUDAgIeAQNDAARAl8vdQt+A
KBOymRFka+E4EgIfboNfszWxSBXgQ812JG2NcFIQuGFHQM/iMU5UUTnVzyO7JEdZJy/XnfRCqMTd
nKOBxzCBxDALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUw5msLvj2/PBi
LIqANd/aYygX7+0wcwYDVR0fBGwwajBooGagZIYwaHR0cDovL3ZvZW5tZWgtZDBmMjg2YS9DZXJ0
RW5yb2xsL01heGltJTIwVUMuY3JshjBmaWxlOi8vXFx2b2VubWVoLWQwZjI4NmFcQ2VydEVucm9s
bFxNYXhpbSBVQy5jcmwwEAYJKwYBBAGCNxUBBAMCAQAwCAYGKoUDAgIDA0EAwXTg/ChvhJy6+iTt
o6vRRJfU4kZ0wtSeufgbUxyYuqqV2+vadqJFLwWZ8Zazny/xceUSZsvrWTky9Xtq0Hz4rTB6MSMw
IQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUxDzANBgNVBAcT
Bk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQcm9tbzERMA8GA1UEAxMITWF4
aW0gVUOgfDB6MSMwIQYJKoZIhvcNAQkBFhRtaXZhbm92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMC
UlUxDzANBgNVBAcTBk1vc2NvdzESMBAGA1UEChMJQ3J5cHRvUHJvMQ4wDAYDVQQLEwVQcm9tbzER
MA8GA1UEAxMITWF4aW0gVUMCEAdIusWQ6sWbTE8P5wSYnKinggN4oIIDdKGCA3AwEAwLQ1JMIGZy
b20gQ0EDAQAwDQYLKwYBBAHoAIN3AQKhggNLBgsrBgEEAegAg3cBAqCCAzowggM2BAQAAAABoHww
ejEjMCEGCSqGSIb3DQEJARYUbWl2YW5vdkBmYWN0b3ItdHMucnUxCzAJBgNVBAYTAlJVMQ8wDQYD
VQQHEwZNb3Njb3cxEjAQBgNVBAoTCUNyeXB0b1BybzEOMAwGA1UECxMFUHJvbW8xETAPBgNVBAMT
CE1heGltIFVDMIICrjCCAl0CAQEwCAYGKoUDAgIDMHoxIzAhBgkqhkiG9w0BCQEWFG1pdmFub3ZA
ZmFjdG9yLXRzLnJ1MQswCQYDVQQGEwJSVTEPMA0GA1UEBxMGTW9zY293MRIwEAYDVQQKEwlDcnlw
dG9Qcm8xDjAMBgNVBAsTBVByb21vMREwDwYDVQQDEwhNYXhpbSBVQxcNMTIwNTE1MDkxMDA2WhcN
MTIwNTIyMjEzMDA2WjCBgTApAgphBNZnAAAAAAASFw0xMjA1MDIxMTQxMjdaMAwwCgYDVR0VBAMK
AQUwKQIKYRBfpgAAAAABxcNMTIwNTAyMTEzODIwWjAMMAoGA1UdFQQDCgEFMCkCCmHpQqkAAAAA
ABEXDTEyMDUwMjExMzgwNVowDDAKBgNVHRUEAwoBBaCCAS4wggEqMB8GA1UdIwQYMBaAFMOZrC74

9vzwYiyKgDXf2mMoF+/tMBAGCSsGAQQBgjcVAQQDAgEAMAoGA1UdFAQDAgEFMBwGCSsGAQQBgjcV
BAQPFw0xMjA1MjIwOTIwMDZaMIHKBgkrBgEEAYI3FQ4EgbwwgbkwgbaggbOggbCGga1sZGFwOi8v
L0NOPU1heGltJTIwVUMsQ049dm9lbm1laC1kMGYyODZhLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxEQz1VbmF2YWlsYWJsZUNvbmZpZ0ROP2NlcnRpZmljYXRl
UmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDAIBgYq
hQMCAgMDQQBwtkKKmuMFgp5/W5eharGE+/gj5/LNAqMCkuhTg49R9IikDDfGnTxLqww6oQwLfwI1
AneI0qME/Wfsm5Kwg6tXoIICJ6CCAiO7ggIfMCMMHVByaXZhdGUgS2V5IG9mIEFuZHJleSBGZWRv
dG92AwIHgDAxBAQAAAACAwMGZEADAgXgGA8yMDEyMDUxODExMDMwMFqADzIwMTMwNTE4MTExMjAw
WqCBvTCBujEjMCEGCSqGSIb3DQEJARYUZmVkb3RvdkBmYWN0b3ItdHMucnUxCzAJBgNVBAYTAlJV
MRUwEwYDVQQHHgwEHAQ+BEEEOgQyBDAxGzAZBgNVBAoeEgQkBDAEOgRCBD4EQAAtBCIEITERMA8G
A1UECx4IBCIENQRBBEIxPzA9BgNVBAMeNgQkBDUENAQ+BEIEPgQyACAEEAQ9BDQEQAQ1BDkAIAQS
BDsEMAQ0BDgEPAQ4BEAEPgQyBDgER6GCAQOigfUCAQIxWaJXAgEEMAYEBAAAAAUwHgYHKoUDAgIN
ATATBgcqhQMCAh8BBAj+eDWftOAlsQQqMCgEICDlUBEQHltnpiNOSNa4Q2dQnXwZJOrnMuG70VxM
72D9BATXF9f1MIGUBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIwEwQItA025Kp0vQkGByqFAwICHwGA
ZkavznRD37azfHnu+crVVbSwVsPlv8YGzYFg48u/Ab5mWeuFfP7gJ5s4tfhJBKWBThkn8VjonlJ0
SOhZUaS2DetnIUBQP2696DGiUNMQsGBGXnEOSyasz3C/SOjGdz05lO6yxhk28DAJBgcqhQMCAiMB
pIIFQqCCBT4wggU6MCIMHUNlcnRpZmljYXRlIG9mIEFuZHJleSBGZWRvdG92AwEAMAYEBAAAAAKh
ggUKoIIDvzCCA26gAwIBAgIKYUp2IgAAAAAAHTAIBgYqhQMCAgMwejEjMCEGCSqGSIb3DQEJARYU
bWl2YW5vdkBmYWN0b3ItdHMucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxEjAQBgNV
BAoTCUNyeXB0b1BybzEOMAwGA1UECxMFUHJvbW8xETAPBgNVBAMTCE1heGltIFVDMB4XDTEyMDUx
ODExMDMwMFoXDTEzMDUxODExMTIwMFowgboxIzAhBgkqhkiG9w0BCQEWFGZlZG90b3ZAZmFjdG9y
LXRzLnJ1MQswCQYDVQQGEwJSVTEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMRswGQYDVQQKHhIEJAQw
BDoEQgQ+BEAALQQiBCExETAPBgNVBAseCAQiBDUEQQRCMT8wPQYDVQQDHjYEJAQ1BDQEPgRCBD4E
MgAgBBAEPQQ0BEAENQQ5ACAEEgQ7BDAENAQ4BDwEOARABD4EMgQ4BEcwYzAcBgYqhQMCAhMwEgYH
KoUDAgIjAQYHKoUDAgIeAQNDAARA7ZIDZgAQEbmsMmgoVnaV0kuxHyJmgvxTzJHKagoUMGcnalND
0eKTFkshABKJR8iG+SFElVEIp0XmF4VzdZ1kTqOCAZEwggGNMA4GA1UdDwEB/wQEAwIE8DATBgNV
HSUEDDAKBggrBgEFBQgCAjAdBgNVHQ4EFgQUUlitDEVDDeX23jl7dzs9+R1p/zkwHwYDVR0jBBgw
FoAUw5msLvj2/PBiLIqANd/aYygX7+0wdQYDVR0fBG4wbDBqoGigZoYwaHR0cDovL3ZvZW5tZWgt
ZDBmMjg2YS9DZXJ0RW5yb2xsL01heGltJTIwVUMuY3JshjJmaWxlOi8vXFx2b2VubWVoLWQwZjI4
NmFcQ2VydEVucm9sbFxNYXhpbSUyMFVDLmNybDCBrgYIKwYBBQUHAQEEgaEwgZ4wTAYIKwYBBQUH
MAKGQGh0dHA6Ly92b2VubWVoLWQwZjI4NmEvQ2VydEVucm9sbC92b2VubWVoLWQwZjI4NmFfTWF4
aW0lMjBVQy5jcnQwTgYIKwYBBQUHMAKGQmZpbGU6Ly9cXHZvZW5tZWgtZDBmMjg2YVxDZXJ0RW5y
b2xsXHZvZW5tZWgtZDBmMjg2YV9NYXhpbSUyMFVDLmNydDAIBgYqhQMCAgMDQQBx2yNnJZzJ0IYq
yR3ZnarIUbypLLr0gvP0js8MgXenLzU0itibsbAKGFCifs+KbcteUyGICOzzyno2Ao2i8fXkMIG6
MSMwIQYJKoZIhvcNAQkBFhRmZWRvdG92QGZhY3Rvci10cy5ydTELMAkGA1UEBhMCUlUxFTATBgNV
BAceDAQcBD4EQQQ6BDIEMDEbMBkGA1UECh4SBCQEMAQ6BEIEPgRAAC0EIgQhMREwDwYDVQQLHggE
IgQ1BEEEQjE/MD0GA1UEAx42BCQENQQ0BD4EQgQ+BDIAIAQQBD0ENARABDUEOQAgBBIEOwQwBDQE
OAQ8BDgEQAQ+BDIEOARHoHwwejEjMCEGCSqGSIb3DQEJARYUbWl2YW5vdkBmYWN0b3ItdHMucnUx
CzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cxEjAQBgNVBAoTCUNyeXB0b1BybzEOMAwGA1UE
CxMFUHJvbW8xETAPBgNVBAMTCE1heGltIFVDAgphSnYiAAAAAAAdoIIBQKCCATy7ggE4MB8MGU5l
dyBHZW5lcmF0ZWQgUHJpdmF0ZSBLZXkDAgeAMA4EBAAAAAMDAgUgAwIF4KGCAQOigfUCAQIxWaJX
AgEEMAYEBAAAAAUwHgYHKoUDAgINATATBgcqhQMCAh8BBAgVtDwYK241mAQqMCgEIHTaHqSIEbop
HC9V/0zdoiJxJ5+2M4+sBjZypmOFsn5SBASOnnw0MIGUBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIw
EwQI+cwk4q5mKEkGByqFAwICHwGAZjrP51hTaeVJGh1MlSLpQ//xh9wQbqm9NJ2rZDRXmopNTNTD
m4rhVjsg0m6xfZmsYdiIwntBYxvO2zp1q4psXF8emiw8NUGnMyRH4k1BL0vNdghwv9ord/Vrao/+
NXBBYC4j22pNYjAJBgcqhQMCAiMCoYGSoIGPu4GMMC0MKFB1YmxpYyBLZXkgZm9yIE5ldyBHZW5l
cmF0ZWQgUHJpdmF0ZSBLZXkDAQAwCgQEAAAAAwMCAQKhT6BCBEAei879fJXoTxHjWhSgWP1byz4k
iTrekVmZ6ydbo6+vHdTVjWwyomTTiubNB1QMdntBXmRUC+kjAqf06vplzfZLMAkGByqFAwICIwKg
ggHBoIIBvbuCAbkwGQwTNTEyLWJpdCBwcml2YXRlIGtleQMCB4AwMAQEAAAABAMCBSADAgXgGA8y
MDEzMTAyMjEyMTQzM1qADzIwMTQxMDE4MjIwMDAwWqGCAWiiggFXAgECMVmiVwIBBDAGBAQAAAAF
MB4GByqFAwICDQEwEwYHKoUDAgIfAQQIQll6v0b62SQEKjAoBCCG/ACAyQcxLWULxpO4Nz/6w7vP
DCqpFcCevwQfDfWx7QQE42g82DCB9gYJKoZIhvcNAQcBMB8GCCqFAwIEAwICMBMECPi1cO7kvILE
BgcqhQMCAh8BgIHHSAzMW3SKRLx1gyLSz2irGpx0zHh+Q4jr6JwtFcLLvOh2NbrtxUruxWAnOjDc
CpR0kJI5s4ilnP5ZRF+qKw8Z0VLKcYme2GzZPtla+1LjZ2aVI1JQ19kQh3kbG8IMPbzZyYN2StXS
9TTPVsoGA6BUXa+xZcbgg3WroEK08GnD8E5rfZc3Zmjeubx0u+JkIFH/6l0MIXJbCU7178N8BCTc
EVzP+8xJ8vJ0T4Kn/EmlxNQzpCUsrcfTXmZ31xSlKgnxQSl72zA2sTALBgkqhQMHAQIBAgChgf0g
gfC7ge0wJwwiUHVibGljIGtleSBmb3IgNTEyLWJpdCBwcml2YXRlIGtleQMBADAsBAQAAAAEAwIB
AhgPMjAxMzEwMjIxMjE0MzNagA8yMDE0MTAxODIyMDAwMFqhgZOggYMEgYAP6sVXoKYw7qylOhzL
yUhtweEAjcu6rcm3f4v+lDLB0gnahQ1AjRwXIaxTNjR+pEDMJ6SbrboFWPWdkAkrSzkeC988Zpnq
6SUXE+Ge+P6sOTsmlBoIuszncdADJKBnNqTtKHshB5AycqoYOLrDvVFrnCoi2+7KuLFfEtsaoXT5
AzALBgkqhQMHAQIBAgCnggEgoIIBHKGCARgwFQwPVG9wLXNlY3JldCBEYXRhAwIGwDANBgsrBgEE

AegAg3cBBKGB7wYFKYNIvVKigeUCAQIxWaJXAgEEMAYEBAAAAAUwHgYHKoUDAgINATATBgcqhQMC
Ah8BBAiRUP442GWxSQQqMCgEIEreeRUx8RT4pxDjbItscBL+VFX+kwe1qHN+KMP0C2xlBASMXaf0
MIGEBgkqhkiG9w0BBwEwHwYIKoUDAgQDAgIwEwQIVhCwc1AB2HcGByqFAwICHwGAVrSgjIpwdcaL
sbCdixi7oaLiKz6wtb3G1pfDa49FRgGAI9vrUdfXXEocym83zZXIUyoQupvqCU3SGkzJSUKyES1/
GhlN6MXICVUj5Xgo9gY7dT+Ns2lsp2ugaaFnMBEMC1B1YmxpYyBEYXRhAwIGQDANBgsrBgEEAegA
g3cBBKFDBgYphX2DMAGgOQQ3VGhpcyBpcyBzb21lIG9wZW4gZGF0YS4gVGhlcmUncyBubyBuZWVk
IHRvIGVuY3J5cHQgaXQuAKJsMBkGCSqGSIb3DQEJAzEMBgoqhkiG9w0BDwMBME8GCSqGSIb3DQEJ
BDFCBEBzSiqsP0NER7o3sxCuY5PBk5DseIncZjd33xbaJKBBY3sve6CEo5MJCNcsB7yTbF+NzueC
rDuxV2ajsbUcUvY+BEAmPK+zDst16Hbso4uj0md4BQZj6aOIZ3kSrrrRDkpdWJd/87jXAIoK3Tiv
Czjk8sNQ9RWnbnX0ijv1bvTOI6m6

Процесс формирования контейнера:

```
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 (1-8 - cproA,B,C,XchA,XchB,512test,512A,512B): 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  |0gost.e-ecolog.ru |
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..@gost.e-ecolog.ru
```

```
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 (1-8 - cproA,B,C,XchA,XchB,512test,512A,512B): 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 (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 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_private_key: Adding key '512-bit private key':
key usage: SIGN
key access: SENSITIVE EXTRACTABLE ALWAYSSENSITIVE
key parameters (1-8 - cproA,B,C,XchA,XchB,512test,512A,512B): 6
start date: 2013-10-22 12:14:33
end date: 2014-10-18 22:00:00
key (little-endian):
38 02 3C F1  7E 36 6C DC  A6 B0 17 8B  84 05 0F 07  |8.<.~6l.........|
D5 1D F5 30  63 0C 49 64  C4 CE D7 72  07 07 FD B1  |...0c.Id...r....|
60 61 0E 1B  D6 A7 C2 EE  89 4D 01 99  59 D2 98 20  |`a.......M..Y.. |
5B 1D 6B 62  7D F4 B3 83  5A 80 81 34  CD 80 4B 2D  |[.kb}...Z..4..K-|
```

```
Remasking private key '512-bit private key':
Unmasked key (little-endian):
38 02 3C F1  7E 36 6C DC  A6 B0 17 8B  84 05 0F 07  |8.<.~6l.........|
D5 1D F5 30  63 0C 49 64  C4 CE D7 72  07 07 FD B1  |...0c.Id...r....|
60 61 0E 1B  D6 A7 C2 EE  89 4D 01 99  59 D2 98 20  |`a.......M..Y.. |
5B 1D 6B 62  7D F4 B3 83  5A 80 81 34  CD 80 4B 2D  |[.kb}...Z..4..K-|
Masked key (little-endian):
F4 3E C1 61  62 CA 43 77  85 BB 72 17  86 6F 29 E7  |.>.ab.Cw..r..o).|
1B 9E 3B FD  99 7C BB CE  89 BA 15 9F  5D 5B 63 C6  |..;..|......][c.|
85 9E E2 33  7F BA D0 2B  5F B1 D3 39  01 AB 2A AC  |...3...+_..9..*.|
40 B6 45 DB  F9 73 F9 30  89 CA 84 3B  2B B6 DF 06  |@.E..s.0...;+...|
Mask 1:
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..?...|
2D 97 B7 91  F9 AE B6 DC  AF C2 F3 9F  7A 34 5E 20  |-...........z4^ |
2A B0 FE 1E  C2 62 63 3B  2E 5F 1F 1B  9A 7F 58 7C  |*....bc;._....X||
Mask 2:
8A D0 00 FB  06 40 32 4D  DF 2F 70 F7  EB 78 D3 84  |.....@2M./p..x..|
5D 47 47 36  72 A7 05 37  A2 14 A9 61  CB 1A 49 59  |]GG6r..7...a..IY|
53 59 7F 76  E1 D8 C4 D7  9A AA FB 7E  9D 1A 83 F8  |SY.v.......~....|
98 24 78 92  87 AB F0 97  EB 7C 32 02  D4 E9 28 50  |.$x......|2...(P|

p15_add_public_key: Adding key 'Public key for 512-bit private key'
key usage: VERIFY
key parameters (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 6
start date: 2013-10-22 12:14:33
end date: 2014-10-18 22:00:00
key (little-endian):
0F EA C5 57  A0 A6 30 EE  AC A5 3A 1C  CB C9 48 6D  |...W..0...:...Hm|
C1 E1 00 8D  CB BA AD C9  B7 7F 8B FE  94 32 C1 D2  |.............2..|
09 DA 85 0D  40 8D 1C 17  21 AC 53 36  34 7E A4 40  |....@...!.S64~.@|
CC 27 A4 9B  AD BA 05 58  F5 9D 90 09  2B 4B 39 1E  |.'.....X....+K9.|
0B DF 3C 66  99 EA E9 25  17 13 E1 9E  F8 FE AC 39  |..<f...%.......9|
3B 26 94 1A  08 BA CC E7  71 D0 03 24  A0 67 36 A4  |;&......q..$.g6.|
ED 28 7B 21  07 90 32 72  AA 18 38 BA  C3 BD 51 6B  |.({!..2r..8...Qk|
9C 2A 22 DB  EE CA B8 B1  5F 12 DB 1A  A1 74 F9 03  |.*".....____.t..|

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 (HMAC-
GOST3411-2012).
Input password:
31 32 33                                            |123              |
Iteration count: 2000
```

```
Salt:
74 BA EE A0  BE CB 77 5E  4E C9 BA B5  2E 01 4A A0  |t.....w^N.....J.|
EE DF F0 96  80 14 53 6A  8E F4 1B CB  76 F4 D3 E3  |......Sj....v...|
Generated password key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|

Making KEKRecipientInfo for AuthenticatedData:
kekri.kekid.keyIdentifier:
00 00 00 05                                        |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
C9 26 33 3D  94 AB 69 C4                           |.&3=..i.        |
Key wrap:
Pw key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|
Session key:
CA 0F C3 47  47 09 52 F5  82 06 7D 0A  7A A8 49 08  |...GG.R...}.z.I.|
C7 6D 3C 2F  F8 9C 3B C3  09 31 3B 2A  61 B3 46 F5  |.m</..;..1;*a.F.|
Wrapped key:
D4 5E 3C 08  23 1B BF 4A  6A F5 3F 7F  63 F4 1E 77  |.^<.#..Jj.?.c..w|
45 D6 4E 51  63 56 E3 30  52 FB F9 D0  C2 D5 48 EB  |E.NQcV.0R.....H.|
MAC of key:
B4 F9 39 3F                                        |..9?            |
kekri.encryptedKey content:
30 28 04 20  D4 5E 3C 08  23 1B BF 4A  6A F5 3F 7F  |0(. .^<.#..Jj.?.|
63 F4 1E 77  45 D6 4E 51  63 56 E3 30  52 FB F9 D0  |c..wE.NQcV.0R...|
C2 D5 48 EB  04 04 B4 F9  39 3F                    |..H.....9?      |

AuthenticatedData.macAlgorithm.algorithm: 1.2.643.7.1.1.4.2
AuthenticatedData.digestAlgorithm.algorithm: 1.2.643.7.1.1.2.3
AuthenticatedData.encapContentInfo.eContentType: 1.2.840.113549.1.15.3.1

Making PKCS15Token:

token.keyManagementInfo.keyId:
00 00 00 05                                        |....            |
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:
74 BA EE A0  BE CB 77 5E  4E C9 BA B5  2E 01 4A A0  |t.....w^N.....J.|
EE DF F0 96  80 14 53 6A  8E F4 1B CB  76 F4 D3 E3  |......Sj....v...|
par.iterationCount:
07 D0                                              |..              |
par.keyLength: 32
par.prf.algorithm: 1.2.643.7.1.1.4.2
token.keyManagementInfo.keyInfo.passwordInfo.algId.parameters (encoded):
30 35 04 20  74 BA EE A0  BE CB 77 5E  4E C9 BA B5  |05. t.....w^N...|
2E 01 4A A0  EE DF F0 96  80 14 53 6A  8E F4 1B CB  |..J.......Sj....|
76 F4 D3 E3  02 02 07 D0  02 01 20 30  0A 06 08 2A  |v......... 0...*|
85 03 07 01  01 04 02                              |.......         |

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: 4
FactorTSVersion.minorVersion: 0
Encoded oidDO.typeAttributes.value.direct:
30 06 02 01  04 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:
F6 9F A8 86  2D 52 C1 8E  3B A6 CC 87  65 BB 7B 0C  |....-R..;...e.{.|
74 70 70 52  12 2A 80 50  DD 8E C8 00  0F CA 11 88  |tppR.*.P........|
D7 DF B8 19  83 EA FF C1  09 B4 ED 5C  F2 CA 61 00  |...........\..a.|
3B 3D B4 C5  38 60 01 84  D1 50 82 15  14 EE 9F F6  |;=..8`...P......|
RandomInitValue.moreRandom:
56 03 1D 59  14 76 D5 DC  B9 E1 11 6E  7D 94 8C     |V..Y.v.....n}.. |
Encoded RandomInitValue:
30 53 04 40  F6 9F A8 86  2D 52 C1 8E  3B A6 CC 87  |0S.@....-R..;...|
65 BB 7B 0C  74 70 70 52  12 2A 80 50  DD 8E C8 00  |e.{.tppR.*.P....|
0F CA 11 88  D7 DF B8 19  83 EA FF C1  09 B4 ED 5C  |...............\|
F2 CA 61 00  3B 3D B4 C5  38 60 01 84  D1 50 82 15  |..a.;=..8`...P..|
14 EE 9F F6  04 0F 56 03  1D 59 14 76  D5 DC B9 E1  |......V..Y.v....|
11 6E 7D 94  8C                                      |.n}..           |
Making EnvelopedData of RandomInitValue:
p15_mk_enveloped_data: Making EnvelopedData.recipientInfos (1 kekri):
kekri.kekid.keyIdentifier:
00 00 00 05                                          |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
F0 86 00 8A  B4 17 5A F7                             |......Z.        |
Key wrap:
Pw key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|
Session key:
74 D1 B8 53  64 3F A0 01  54 E0 E8 3D  AF 19 1C B3  |t..Sd?..T..=....|
9D 20 91 56  1B 07 5C 46  5C 55 6A 5B  B3 15 45 2D  |. .V..\F\Uj[..E-|
Wrapped key:
F3 73 D2 4D  08 DD 75 69  8B 78 DB 8A  30 7C 90 F0  |.s.M..ui.x..0|..|
7D E2 44 DD  EE AC 88 81  9B 60 92 1D  B4 55 4C 8C  |}.D......`...UL.|
MAC of key:
4B 66 2E 58                                          |Kf.X            |
kekri.encryptedKey content:
30 28 04 20  F3 73 D2 4D  08 DD 75 69  8B 78 DB 8A  |0(. .s.M..ui.x..|
30 7C 90 F0  7D E2 44 DD  EE AC 88 81  9B 60 92 1D  |0|..}.D......`..|
B4 55 4C 8C  04 04 4B 66  2E 58                      |.UL...Kf.X      |
```

```
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
D7 AA B1 2C  32 BD AC 80                                |...,2...        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  D7 AA B1 2C  32 BD AC 80  06 07 2A 85  |0......,2.....*.|
03 02 02 1F  01                                         |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
5E C3 5B B2  64 BE A1 09  1D 8C 01 D8  2F B7 7A 4D  |^.[.d......./.zM|
89 AA 0D 00  93 74 38 82  2C CB 2E F1  E1 D5 7E B0  |.....t8.,.....~.|
21 25 DB 01  6E 16 00 70  85 DB 15 7B  69 5D 2E 91  |!%..n..p...{i]..|
50 AB 9A A6  60 EE 95 6B  5F CF E5 E4  6C EF 73 C9  |P...`..k_...l.s.|
62 DF 45 B9  AE 27 48 DF  0D D3 92 97  AB 88 BB 71  |b.E..'H........q|
CB 11 43 A0  5C 58 1A E8  E1                        |..C.\X...       |


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):
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).
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_2012Key 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 05                                         |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
FE 78 35 9F  B4 E0 25 B1                            |.x5...%.        |
Key wrap:
Pw key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|
Session key:
```

```
B5 64 68 9B  6B 3F 1D B9  A2 A3 99 88  7B 60 6B 61  |.dh.k?......{`ka|
53 C1 87 84  0D CB 67 F9  A4 AB BC 90  3D 41 D4 8C  |S.....g.....=A..|
Wrapped key:
20 E5 50 11  10 1E 5B 67  A6 23 4E 48  D6 B8 43 67  | .P...[g.#NH..Cg|
50 9D 7C 19  24 EA E7 32  E1 BB D1 5C  4C EF 60 FD  |P.|.$..2...\L.`.|
MAC of key:
D7 17 D7 F5                                        |....            |
kekri.encryptedKey content:
30 28 04 20  20 E5 50 11  10 1E 5B 67  A6 23 4E 48  |0(.  .P...[g.#NH|
D6 B8 43 67  50 9D 7C 19  24 EA E7 32  E1 BB D1 5C  |..CgP.|.$..2...\|
4C EF 60 FD  04 04 D7 17  D7 F5                    |L.`.......      |

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
B4 0D 36 E4  AA 74 BD 09                           |..6..t..        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  B4 0D 36 E4  AA 74 BD 09  06 07 2A 85  |0.....6..t....*.|
03 02 02 1F  01                                    |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
46 AF CE 74  43 DF B6 B3  7C 79 EE F9  CA D5 55 B4  |F..tC...|y....U.|
B0 56 C3 E5  BF C6 06 CD  81 60 E3 CB  BF 01 BE 66  |.V.......`.....f|
59 EB 85 7C  FE E0 27 9B  38 B5 F8 49  04 A5 81 4E  |Y..|..'.8..I...N|
19 27 F1 58  E8 9E 52 74  48 E8 59 51  A4 B6 0D EB  |.'.X..RtH.YQ....|
67 21 40 50  3F 6E BD E8  31 A2 50 D3  10 B0 60 46  |g!@P?n..1.P...`F|
5E 71 0E 4B  26 AC CF 70  BF 48 E8 C6  77 3D 39 94  |^q.K&..p.H..w=9.|
EE B2 C6 19  36 F0                                 |....6.          |

Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.gostR3410-2012ParamSet (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 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   |
6E 64 72 65  79 20 46 65  64 6F 74 6F  76           |Andrey 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).
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_2012Key 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 05                                         |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
15 B4 3C 18  2B 6E 35 98                            |..<.+n5.        |
Key wrap:
Pw key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|
Session key:
C8 B8 8B E0  B3 67 67 0F  64 8D FD D1  D9 96 F8 3F  |.....gg.d......?|
AF 03 53 71  14 3F AF 52  D7 68 FA B8  B7 0B BB E9  |..Sq.?.R.h......|
Wrapped key:
74 DA 1E A4  88 11 BA 29  1C 2F 55 FF  4C DD A2 22  |t......)./U.L.."|
71 27 9F B6  33 8F AC 06  36 72 A6 63  85 B2 7E 52  |q'..3...6r.c..~R|
MAC of key:
8E 9E 7C 34                                         |..|4            |
kekri.encryptedKey content:
30 28 04 20  74 DA 1E A4  88 11 BA 29  1C 2F 55 FF  |0(. t......)./U.|
4C DD A2 22  71 27 9F B6  33 8F AC 06  36 72 A6 63  |L.."q'..3...6r.c|
85 B2 7E 52  04 04 8E 9E  7C 34                      |..~R....|4      |

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
F9 CC 24 E2  AE 66 28 49                              |..$..f(I        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  F9 CC 24 E2  AE 66 28 49  06 07 2A 85  |0.....$..f(I..*.|
03 02 02 1F  01                                      |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
3A CF E7 58  53 69 E5 49  1A 1D 4C 95  22 E9 43 FF  |:..XSi.I..L.".C.|
F1 87 DC 10  6E A9 BD 34  9D AB 64 34  57 9A 8A 4D  |....n..4..d4W..M|
4C D4 C3 9B  8A E1 56 3B  20 D2 6E B1  7D 99 AC 61  |L.....V; .n.}..a|
D8 88 C2 7B  41 63 1B CE  DB 3A 75 AB  8A 6C 5C 5F  |...{Ac...:u..l\_|
1E 9A 2C 3C  35 41 A7 33  24 47 E2 4D  41 2F 4B CD  |..,<5A.3$G.MA/K.|
76 08 70 BF  DA 2B 77 F5  6B 6A 8F FE  35 70 41 60  |v.p..+w.kj..5pA`|
2E 23 DB 6A  4D 62                                   |.#.jMb          |

Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.gostR3410-2012ParamSet (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 2

Adding token.pkcs15Objects.publicKeys element:

p15_mk_pubkey_obj: Making public key 'Public Key for New Generated Private Key'
object:
Choosing PublicKeyType.publicGostR3410_2012Key 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.
GostR3410Point (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.gostR3410-2012ParamSet (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 2

Adding token.pkcs15Objects.privateKeys element:

p15_mk_prkey_obj: Making private key '512-bit private key' object:
Choosing PrivateKeyType.privateGostR3410_2012Key choice.
key.commonObjectAttributes.label:
35 31 32 2D  62 69 74 20  70 72 69 76  61 74 65 20  |512-bit private |
6B 65 79                                             |key             |
key.commonObjectAttributes.flags: 0x80, len=1, unused_bits=6
key.classAttributes.iD:
00 00 00 04                                          |....            |
key.classAttributes.usage: len=2, unused_bits=6:
20                                                   |                |
key.classAttributes.accessFlags: len=1, unused_bits=3: 0xE0
key.classAttributes.startDate:
32 30 31 33  31 30 32 32  31 32 31 34  33 33 5A     |20131022121433Z |
key.classAttributes.endDate:
32 30 31 34  31 30 31 38  32 32 30 30  30 30 5A     |20141018220000Z |
```

```
Encoded GostPrivateKey (195 bytes):
04 81 C0 F4  3E C1 61 62  CA 43 77 85  BB 72 17 86  |....>.ab.Cw..r..|
6F 29 E7 1B  9E 3B FD 99  7C BB CE 89  BA 15 9F 5D  |o)...;..|......]|
5B 63 C6 85  9E E2 33 7F  BA D0 2B 5F  B1 D3 39 01  |[c....3...+_..9.|
AB 2A AC 40  B6 45 DB F9  73 F9 30 89  CA 84 3B 2B  |.*.@.E..s.0...;+|
B6 DF 06 F4  53 80 45 B0  2F C8 C6 DE  AA 01 ED A5  |....S.E./.......|
16 21 DD B1  65 FB 1F 53  AB C9 4C 1D  64 B3 BD 3F  |.!..e..S..L.d..?|
D9 D8 0C 2D  97 B7 91 F9  AE B6 DC AF  C2 F3 9F 7A  |...-...........z|
34 5E 20 2A  B0 FE 1E C2  62 63 3B 2E  5F 1F 1B 9A  |4^ *....bc;._...|
7F 58 7C 8A  D0 00 FB 06  40 32 4D DF  2F 70 F7 EB  |.X|.....@2M./p..|
78 D3 84 5D  47 47 36 72  A7 05 37 A2  14 A9 61 CB  |x..]GG6r..7...a.|
1A 49 59 53  59 7F 76 E1  D8 C4 D7 9A  AA FB 7E 9D  |.IYSY.v.......~.|
1A 83 F8 98  24 78 92 87  AB F0 97 EB  7C 32 02 D4  |....$x......|2..|
E9 28 50                                           |.(P             |
Wrapping  GostPrivateKey  to  EnvelopedData  (key.typeAttributes.value.direct-
protected:
p15_mk_enveloped_data: Making EnvelopedData.recipientInfos (1 kekri):
kekri.kekid.keyIdentifier:
00 00 00 05                                        |....            |
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
42 59 7A BF  46 FA D9 24                           |BYz.F..$        |
Key wrap:
Pw key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|
Session key:
8C 35 96 F6  3E CF 3A 2F  70 9A E7 FC  15 91 02 90  |.5..>.:/p.......|
B9 10 04 9F  E5 C7 EF 1F  F2 99 45 D0  74 B9 4F 14  |..........E.t.O.|
Wrapped key:
86 FC 00 80  C9 07 31 2D  65 0B C6 93  B8 37 3F FA  |......1-e....7?.|
C3 BB CF 0C  2A A9 15 C0  9E BF 04 1F  0D F5 B1 ED  |....*...........|
MAC of key:
E3 68 3C D8                                        |.h<.            |
kekri.encryptedKey content:
30 28 04 20  86 FC 00 80  C9 07 31 2D  65 0B C6 93  |0(. ......1-e...|
B8 37 3F FA  C3 BB CF 0C  2A A9 15 C0  9E BF 04 1F  |.7?.....*.......|
0D F5 B1 ED  04 04 E3 68  3C D8                    |.......h<.      |

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
F8 B5 70 EE  E4 BC 82 C4                           |..p.....        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  F8 B5 70 EE  E4 BC 82 C4  06 07 2A 85  |0.....p.......*.|
03 02 02 1F  01                                    |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
48 0C CC 5B  74 8A 44 BC  75 83 22 D2  CF 68 AB 1A  |H..[t.D.u."..h..|
9C 74 CC 78  7E 43 88 EB  E8 9C 2D 15  C2 CB BC E8  |.t.x~C....-.....|
76 35 BA ED  C5 4A EE C5  60 27 3A 30  DC 0A 94 74  |v5...J..`':0...t|
90 92 39 B3  88 A5 9C FE  59 44 5F AA  2B 0F 19 D1  |..9.....YD_.+...|
52 CA 71 89  9E D8 6C D9  3E D9 5A FB  52 E3 67 66  |R.q...l.>.Z.R.gf|
95 23 52 50  D7 D9 10 87  79 1B 1B C2  0C 3D BC D9  |.#RP....y....=..|
C9 83 76 4A  D5 D2 F5 34  CF 56 CA 06  03 A0 54 5D  |..vJ...4.V....T]|
AF B1 65 C6  E0 83 75 AB  A0 42 B4 F0  69 C3 F0 4E  |..e...u..B..i..N|
```

```
6B 7D 97 37  66 68 DE B9  BC 4E BB E2  64 20 51 FF  |k}.7fh...N..d Q.|
EB 5D 0C 21  72 5B 09 4E  F5 EF C3 7C  04 24 DC 11  |.].!r[.N...|.$..|
5C CF FB CC  49 F2 F2 74  4F 82 A7 FC  49 A5 C4 D4  |\...I..tO...I...|
33 A4 25 2C  AD C7 D3 5E  66 77 D7 14  A5 2A 09 F1  |3.%,...^fw...*..|
41 29 7B DB  30 36 B1                               |A){.06.         |

Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.gostR3410-2012ParamSet (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 6

Adding token.pkcs15Objects.publicKeys element:

p15_mk_pubkey_obj: Making public key 'Public key for 512-bit private key' object:
Choosing PublicKeyType.publicGostR3410_2012Key choice.
key.commonObjectAttributes.label:
50 75 62 6C  69 63 20 6B  65 79 20 66  6F 72 20 35  |Public key for 5|
31 32 2D 62  69 74 20 70  72 69 76 61  74 65 20 6B  |12-bit private k|
65 79                                               |ey              |
key.commonObjectAttributes.flags: 0x00, len=1, unused_bits=6
key.classAttributes.iD:
00 00 00 04                                         |....            |
key.classAttributes.usage: len=2, unused_bits=6:
02                                                  |.               |
key.classAttributes.startDate:
32 30 31 33  31 30 32 32  31 32 31 34  33 33 5A     |20131022121433Z |
key.classAttributes.endDate:
32 30 31 34  31 30 31 38  32 32 30 30  30 30 5A     |20141018220000Z |
Making key.typeAttributes.value:
Choosing key.typeAttributes.value.direct.raw choice.
GostR3410Point (w/o ostr header):
0F EA C5 57  A0 A6 30 EE  AC A5 3A 1C  CB C9 48 6D  |...W..0...:...Hm|
C1 E1 00 8D  CB BA AD C9  B7 7F 8B FE  94 32 C1 D2  |.............2..|
09 DA 85 0D  40 8D 1C 17  21 AC 53 36  34 7E A4 40  |....@...!.S64~.@|
CC 27 A4 9B  AD BA 05 58  F5 9D 90 09  2B 4B 39 1E  |.'.....X....+K9.|
0B DF 3C 66  99 EA E9 25  17 13 E1 9E  F8 FE AC 39  |..<f...%.......9|
3B 26 94 1A  08 BA CC E7  71 D0 03 24  A0 67 36 A4  |;&......q..$.g6.|
ED 28 7B 21  07 90 32 72  AA 18 38 BA  C3 BD 51 6B  |.({!..2r..8...Qk|
9C 2A 22 DB  EE CA B8 B1  5F 12 DB 1A  A1 74 F9 03  |.*"......_....t..|
Making key.typeAttributes.keyInfo.paramsAndOps.parameters:
pars.gostR3410-2012ParamSet (1-8 - cproA,B,C,XchA,XchB,512Test,512A,512B): 6

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 05                                         |....            |
```

```
kekri.keyEncryptionAlgorithm.algorithm: 1.2.643.2.2.13.1
kekri.keyEncryptionAlgorithm.parameters.encryptionParamSet (1-4 = cproA-cproD): 1
kekri.keyEncryptionAlgorithm.parameters.ukm:
91 50 FE 38  D8 65 B1 49                              |.P.8.e.I        |
Key wrap:
Pw key:
6C 5C 3C E5  C6 66 57 6E  9D 7B 63 00  31 B5 85 6C  |l\<..fWn.{c.1..l|
50 AD C8 AA  D9 1E F9 B4  2F 62 F9 0A  45 4E 43 1C  |P......./b..ENC.|
Session key:
97 DF 62 D7  B2 D2 A3 6E  04 02 2D CF  F1 9A C1 AA  |..b....n..-.....|
D7 37 E7 8A  E4 2B EB 6B  66 78 56 E1  37 EB F1 86  |.7...+.kfxV.7...|
Wrapped key:
4A DE 79 15  31 F1 14 F8  A7 10 E3 6C  8B 6C 70 12  |J.y.1......l.lp.|
FE 54 55 FE  93 07 B5 A8  73 7E 28 C3  F4 0B 6C 65  |.TU.....s~(...le|
MAC of key:
8C 5D A7 F4                                           |.]..            |
kekri.encryptedKey content:
30 28 04 20  4A DE 79 15  31 F1 14 F8  A7 10 E3 6C  |0(. J.y.1......l|
8B 6C 70 12  FE 54 55 FE  93 07 B5 A8  73 7E 28 C3  |.lp..TU.....s~(.|
F4 0B 6C 65  04 04 8C 5D  A7 F4                     |..le...]..      |

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
56 10 B0 73  50 01 D8 77                              |V..sP..w        |
par.encryptionParamSet (1-4 - cproA-cproD): 1
Encoded Gost28147-89-Parameters:
30 13 04 08  56 10 B0 73  50 01 D8 77  06 07 2A 85  |0...V..sP..w..*.|
03 02 02 1F  01                                       |.....           |
Making EnvelopedData.encryptedContentInfo.encryptedContent (enc data + imit) :
EnvelopedData.encryptedContentInfo.encryptedContent (w/o ostr header):
B4 A0 8C 8A  70 75 C6 8B  B1 B0 9D 8B  18 BB A1 A2  |....pu..........|
E2 2B 3E B0  B5 BD C6 D6  97 C3 6B 8F  45 46 01 80  |.+>.......k.EF..|
23 DB EB 51  D7 D7 5C 4A  1C CA 6F 37  CD 95 C8 53  |#..Q..\J..o7...S|
2A 10 BA 9B  EA 09 4D D2  1A 4C C9 49  42 B2 11 2D  |*.....M..L.IB..-|
7F 1A 19 4D  E8 C5 C8 09  55 23 E5 78  28 F6 06 3B  |...M....U#.x(..;|
75 3F 8D B3  69 6C                                    |u?..il          |

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) (5855 bytes):
30 82 16 DB  02 01 00 A0  4E 30 4C 04  04 00 00 00  |0.......N0L.....|
05 A0 44 30  42 06 09 2A  86 48 86 F7  0D 01 05 0C  |..D0B..*.H......|
30 35 04 20  74 BA EE A0  BE CB 77 5E  4E C9 BA B5  |05. t.....w^N...|
```

```
2E 01 4A A0  EE DF F0 96  80 14 53 6A  8E F4 1B CB  |..J.......Sj....|
76 F4 D3 E3  02 02 07 D0  02 01 20 30  0A 06 08 2A  |v......... 0...*|
85 03 07 01  01 04 02 30  82 16 84 A7  82 01 6D A0  |.......0......m.|
82 01 69 A1  40 30 16 0C  11 46 61 63  74 6F 72 2D  |..i.@0...Factor-|
54 53 20 76  65 72 73 69  6F 6E 03 01  00 30 0D 06  |TS version...0..|
0B 2B 06 01  04 01 E8 00  83 77 01 03  A1 17 06 0B  |.+.......w......|
2B 06 01 04  01 E8 00 83  77 01 03 A0  08 30 06 02  |+.......w....0..|
01 04 80 01  00 A1 82 01  23 30 17 0C  11 52 61 6E  |........#0...Ran|
64 6F 6D 20  49 6E 69 74  20 56 61 6C  75 65 03 02  |dom Init Value..|
06 C0 30 0D  06 0B 2B 06  01 04 01 E8  00 83 77 01  |..0...+.......w.|
01 A1 81 F8  06 0B 2B 06  01 04 01 E8  00 83 77 01  |......+.......w.|
01 A2 81 E8  02 01 02 31  59 A2 57 02  01 04 30 06  |.......1Y.W...0.|
04 04 00 00  00 05 30 1E  06 07 2A 85  03 02 02 0D  |......0...*.....|
01 30 13 06  07 2A 85 03  02 02 1F 01  04 08 F0 86  |.0...*..........|
00 8A B4 17  5A F7 04 2A  30 28 04 20  F3 73 D2 4D  |....Z..*0(. .s.M|
08 DD 75 69  8B 78 DB 8A  30 7C 90 F0  7D E2 44 DD  |..ui.x..0|..}.D.|
EE AC 88 81  9B 60 92 1D  B4 55 4C 8C  04 04 4B 66  |.....`...UL...Kf|
2E 58 30 81  87 06 09 2A  86 48 86 F7  0D 01 07 01  |.X0....*.H......|
30 1F 06 08  2A 85 03 02  04 03 02 02  30 13 04 08  |0...*.......0...|
D7 AA B1 2C  32 BD AC 80  06 07 2A 85  03 02 02 1F  |...,2.....*.....|
01 80 59 5E  C3 5B B2 64  BE A1 09 1D  8C 01 D8 2F  |..Y^.[.d......./|
B7 7A 4D 89  AA 0D 00 93  74 38 82 2C  CB 2E F1 E1  |.zM.....t8.,....|
D5 7E B0 21  25 DB 01 6E  16 00 70 85  DB 15 7B 69  |.~.!%..n..p...{i|
5D 2E 91 50  AB 9A A6 60  EE 95 6B 5F  CF E5 E4 6C  |]..P...`..k_...l|
EF 73 C9 62  DF 45 B9 AE  27 48 DF 0D  D3 92 97 AB  |.s.b.E..'H......|
88 BB 71 CB  11 43 A0 5C  58 1A E8 E1  A5 82 03 FD  |..q..C.\X.......|
A0 82 03 F9  30 82 03 F5  30 1B 0C 16  52 6F 6F 74  |....0...0...Root|
20 43 65 72  74 69 66 69  63 61 74 65  20 6F 66 20  | Certificate of  |
43 41 03 01  00 30 09 04  04 00 00 00  01 01 01 FF  |CA...0..........|
A1 82 03 C9  A0 82 02 B9  30 82 02 68  A0 03 02 01  |........0..h....|
02 02 10 07  48 BA C5 90  EA C5 9B 4C  4F 0F E7 04  |....H......LO...|
98 9C A8 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 30 1E 17  0D 31 32 30  |.Maxim UC0...120|
33 32 31 31  32 33 39 33  38 5A 17 0D  31 37 30 33  |321123938Z..1703|
32 31 31 32  34 36 31 32  5A 30 7A 31  23 30 21 06  |21124612Z0z1#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 63 30  1C 06 06 2A  85 03 02 02  |im UC0c0...*....|
13 30 12 06  07 2A 85 03  02 02 23 01  06 07 2A 85  |.0...*....#...*.|
03 02 02 1E  01 03 43 00  04 40 97 CB  DD 42 DF 80  |......C..@...B..|
28 13 B2 99  11 64 6B E1  38 12 02 1F  6E 83 5F B3  |(....dk.8...n._.|
35 B1 48 15  E0 43 CD 76  24 6D 8D 70  52 10 B8 61  |5.H..C.v$m.pR..a|
47 40 CF E2  31 4E 54 51  39 D5 CF 23  BB 24 47 59  |G@..1NTQ9..#.$GY|
27 2F D7 9D  F4 42 A8 C4  DD 9C A3 81  C7 30 81 C4  |'/...B.......0..|
30 0B 06 03  55 1D 0F 04  04 03 02 01  86 30 0F 06  |0...U........0..|
03 55 1D 13  01 01 FF 04  05 30 03 01  01 FF 30 1D  |.U.......0....0.|
06 03 55 1D  0E 04 16 04  14 C3 99 AC  2E F8 F6 FC  |..U.............|
F0 62 2C 8A  80 35 DF DA  63 28 17 EF  ED 30 73 06  |.b,..5..c(...0s.|
03 55 1D 1F  04 6C 30 6A  30 68 A0 66  A0 64 86 30  |.U...l0j0h.f.d.0|
```

```
68 74 74 70  3A 2F 2F 76  6F 65 6E 6D  65 68 2D 64  |gost.e-ecolog.ru      |
30 66 32 38  36 61 2F 43  65 72 74 45  6E 72 6F 6C  |0f286a/CertEnrol|
6C 2F 4D 61  78 69 6D 25  32 30 55 43  2E 63 72 6C  |l/Maxim%20UC.crl|
86 30 66 69  6C 65 3A 2F  2F 5C 5C 76  6F 65 6E 6D  |.0file://\\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 4D 61  78 69 6D 20  55 43 2E 63  |nroll\Maxim UC.c|
72 6C 30 10  06 09 2B 06  01 04 01 82  37 15 01 04  |rl0...+.....7...|
03 02 01 00  30 08 06 06  2A 85 03 02  02 03 03 41  |....0...*......A|
00 C1 74 E0  FC 28 6F 84  9C BA FA 24  ED A3 AB D1  |..t..(o....$....|
44 97 D4 E2  46 74 C2 D4  9E B9 F8 1B  53 1C 98 BA  |D...Ft......S...|
AA 95 DB EB  DA 76 A2 45  2F 05 99 F1  96 B3 9F 2F  |.....v.E/....../|
F1 71 E5 12  66 CB EB 59  39 32 F5 7B  6A D0 7C F8  |.q..f..Y92.{j.|.|
AD 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 A0 7C 30  |U....Maxim UC.|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 02  10 07 48 BA  |...Maxim UC...H.|
C5 90 EA C5  9B 4C 4F 0F  E7 04 98 9C  A8 A7 82 03  |.....LO.........|
78 A0 82 03  74 A1 82 03  70 30 10 0C  0B 43 52 4C  |x...t...p0...CRL|
20 66 72 6F  6D 20 43 41  03 01 00 30  0D 06 0B 2B  | from CA...0...+|
06 01 04 01  E8 00 83 77  01 02 A1 82  03 4B 06 0B  |.......w.....K..|
2B 06 01 04  01 E8 00 83  77 01 02 A0  82 03 3A 30  |+.......w.....:0|
82 03 36 04  04 00 00 00  01 A0 7C 30  7A 31 23 30  |..6.......|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  82 02 AE 30  82 02 5D 02  |axim UC0...0..].|
01 01 30 08  06 06 2A 85  03 02 02 03  30 7A 31 23  |..0...*.....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  17 0D 31 32  30 35 31 35  |Maxim UC..120515|
30 39 31 30  30 36 5A 17  0D 31 32 30  35 32 32 32  |091006Z..1205222|
31 33 30 30  36 5A 30 81  81 30 29 02  0A 61 04 D6  |13006Z0..0)..a..|
67 00 00 00  00 00 12 17  0D 31 32 30  35 30 32 31  |g........1205021|
31 34 31 32  37 5A 30 0C  30 0A 06 03  55 1D 15 04  |14127Z0.0...U...|
03 0A 01 05  30 29 02 0A  61 10 5F A6  00 00 00 00  |....0)..a._.....|
00 07 17 0D  31 32 30 35  30 32 31 31  33 38 32 30  |....120502113820|
5A 30 0C 30  0A 06 03 55  1D 15 04 03  0A 01 05 30  |Z0.0...U.......0|
29 02 0A 61  E9 42 A9 00  00 00 00 00  11 17 0D 31  |)..a.B.........1|
32 30 35 30  32 31 31 33  38 30 35 5A  30 0C 30 0A  |20502113805Z0.0.|
06 03 55 1D  15 04 03 0A  01 05 A0 82  01 2E 30 82  |..U...........0.|
```

```
01 2A 30 1F  06 03 55 1D  23 04 18 30  16 80 14 C3  |.*0...U.#..0....|
99 AC 2E F8  F6 FC F0 62  2C 8A 80 35  DF DA 63 28  |.......b,..5..c(|
17 EF ED 30  10 06 09 2B  06 01 04 01  82 37 15 01  |...0...+.....7..|
04 03 02 01  00 30 0A 06  03 55 1D 14  04 03 02 01  |.....0...U......|
05 30 1C 06  09 2B 06 01  04 01 82 37  15 04 04 0F  |.0...+.....7....|
17 0D 31 32  30 35 32 32  30 39 32 30  30 36 5A 30  |..120522092006Z0|
81 CA 06 09  2B 06 01 04  01 82 37 15  0E 04 81 BC  |....+.....7.....|
30 81 B9 30  81 B6 A0 81  B3 A0 81 B0  86 81 AD 6C  |0..0...........l|
64 61 70 3A  2F 2F 2F 43  4E 3D 4D 61  78 69 6D 25  |dap:///CN=Maxim%|
32 30 55 43  2C 43 4E 3D  76 6F 65 6E  6D 65 68 2D  |20UC,CN=voenmeh-|
64 30 66 32  38 36 61 2C  43 4E 3D 43  44 50 2C 43  |d0f286a,CN=CDP,C|
4E 3D 50 75  62 6C 69 63  25 32 30 4B  65 79 25 32  |N=Public%20Key%2|
30 53 65 72  76 69 63 65  73 2C 43 4E  3D 53 65 72  |0Services,CN=Ser|
76 69 63 65  73 2C 44 43  3D 55 6E 61  76 61 69 6C  |vices,DC=Unavail|
61 62 6C 65  43 6F 6E 66  69 67 44 4E  3F 63 65 72  |ableConfigDN?cer |
74 69 66 69  63 61 74 65  52 65 76 6F  63 61 74 69  |tificateRevocati |
6F 6E 4C 69  73 74 3F 62  61 73 65 3F  6F 62 6A 65  |onList?base?obje|
63 74 43 6C  61 73 73 3D  63 52 4C 44  69 73 74 72  |ctClass=cRLDistr|
69 62 75 74  69 6F 6E 50  6F 69 6E 74  30 08 06 06  |ibutionPoint0...|
2A 85 03 02  02 03 03 41  00 70 B6 42  8A 9A E3 05  |*......A.p.B....|
82 9E 7F 5B  97 A1 6A B1  84 FB F8 23  E7 F2 CD 02  |...[..j....#....|
A3 02 92 E8  53 83 8F 51  F4 88 A4 0C  37 C6 9D 3C  |....S..Q....7..<|
4B AB 0C 3A  A1 0C 0B 7F  02 35 02 77  88 D2 A3 04  |K..:.....5.w....|
FD 67 EC 9B  92 B0 83 AB  57 A0 82 02  27 A0 82 02  |.g......W...'...|
23 BB 82 02  1F 30 23 0C  1D 50 72 69  76 61 74 65  |#....0#..Private|
20 4B 65 79  20 6F 66 20  41 6E 64 72  65 79 20 46  | Key of Andrey F|
65 64 6F 74  6F 76 03 02  07 80 30 31  04 04 00 00  |edotov....01....|
00 02 03 03  06 64 40 03  02 05 E0 18  0F 32 30 31  |.....d@......201|
32 30 35 31  38 31 31 30  33 30 30 5A  80 0F 32 30  |20518110300Z..20|
31 33 30 35  31 38 31 31  31 32 30 30  5A A0 81 BD  |1305181112000Z...|
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 A1 82 01  |<.8.@.>.2.8.G...|
03 A2 81 F5  02 01 02 31  59 A2 57 02  01 04 30 06  |.......1Y.W...0.|
04 04 00 00  00 05 30 1E  06 07 2A 85  03 02 02 0D  |......0...*.....|
01 30 13 06  07 2A 85 03  02 02 1F 01  04 08 FE 78  |.0...*.........x|
35 9F B4 E0  25 B1 04 2A  30 28 04 20  20 E5 50 11  |5...%..*0(.  .P.|
10 1E 5B 67  A6 23 4E 48  D6 B8 43 67  50 9D 7C 19  |..[g.#NH..CgP.|.|
24 EA E7 32  E1 BB D1 5C  4C EF 60 FD  04 04 D7 17  |$..2...\L.`.....|
D7 F5 30 81  94 06 09 2A  86 48 86 F7  0D 01 07 01  |..0....*.H......|
30 1F 06 08  2A 85 03 02  04 03 02 02  30 13 04 08  |0...*.......0...|
B4 0D 36 E4  AA 74 BD 09  06 07 2A 85  03 02 02 1F  |..6..t....*.....|
01 80 66 46  AF CE 74 43  DF B6 B3 7C  79 EE F9 CA  |..fF..tC...|y...|
D5 55 B4 B0  56 C3 E5 BF  C6 06 CD 81  60 E3 CB BF  |.U..V.......`...|
01 BE 66 59  EB 85 7C FE  E0 27 9B 38  B5 F8 49 04  |..fY..|..'.8..I.|
A5 81 4E 19  27 F1 58 E8  9E 52 74 48  E8 59 51 A4  |..N.'.X..RtH.YQ.|
B6 0D EB 67  21 40 50 3F  6E BD E8 31  A2 50 D3 10  |...g!@P?n..1.P..|
B0 60 46 5E  71 0E 4B 26  AC CF 70 BF  48 E8 C6 77  |.`F^q.K&..p.H..w|
3D 39 94 EE  B2 C6 19 36  F0 30 09 06  07 2A 85 03  |=9.....6.0...*..|
02 02 23 01  A4 82 05 42  A0 82 05 3E  30 82 05 3A  |..#....B...>0..:|
30 22 0C 1D  43 65 72 74  69 66 69 63  61 74 65 20  |0"..Certificate |
6F 66 20 41  6E 64 72 65  79 20 46 65  64 6F 74 6F  |of Andrey Fedoto|
```

```
76 03 01 00  30 06 04 04  00 00 00 02  A1 82 05 0A  |v...0...........|
A0 82 03 BF  30 82 03 6E  A0 03 02 01  02 02 0A 61  |....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  |0gost.e-ecolog.ru |
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..@gost.e-ecolog.ru
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 30  81 BA 31 23  30 21 06 09  2A 86 48 86  |...0..1#0!..*.H.|
F7 0D 01 09  01 16 14 66  65 64 6F 74  6F 76 40 66  |.......fedotov@f|
61 63 74 6F  72 2D 74 73  2E 72 75 31  0B 30 09 06  |actor-ts.ru1.0..|
03 55 04 06  13 02 52 55  31 15 30 13  06 03 55 04  |.U....RU1.0...U.|
07 1E 0C 04  1C 04 3E 04  41 04 3A 04  32 04 30 31  |......>.A.:.2.01|
1B 30 19 06  03 55 04 0A  1E 12 04 24  04 30 04 3A  |.0...U.....$.0.:|
04 42 04 3E  04 40 00 2D  04 22 04 21  31 11 30 0F  |.B.>.@.-.".!1.0.|
06 03 55 04  0B 1E 08 04  22 04 35 04  41 04 42 31  |..U.....".5.A.B1|
3F 30 3D 06  03 55 04 03  1E 36 04 24  04 35 04 34  |?0=..U...6.$.5.4|
04 3E 04 42  04 3E 04 32  00 20 04 10  04 3D 04 34  |.>.B.>.2. ...=.4|
04 40 04 35  04 39 00 20  04 12 04 3B  04 30 04 34  |.@.5.9. ...;.0.4|
04 38 04 3C  04 38 04 40  04 3E 04 32  04 38 04 47  |.8.<.8.@.>.2.8.G|
A0 7C 30 7A  31 23 30 21  06 09 2A 86  48 86 F7 0D  |.|0z1#0!..*.H...|
01 09 01 16  14 6D 69 76  61 6E 6F 76  40 66 61 63  |.....mivanov@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 0F  30 0D 06 03  55 04 07 13  |....RU1.0...U...|
06 4D 6F 73  63 6F 77 31  12 30 10 06  03 55 04 0A  |.Moscow1.0...U..|
13 09 43 72  79 70 74 6F  50 72 6F 31  0E 30 0C 06  |..CryptoPro1.0..|
03 55 04 0B  13 05 50 72  6F 6D 6F 31  11 30 0F 06  |.U....Promo1.0..|
03 55 04 03  13 08 4D 61  78 69 6D 20  55 43 02 0A  |.U....Maxim UC..|
61 4A 76 22  00 00 00 00  00 1D A0 82  01 40 A0 82  |aJv".........@..|
01 3C BB 82  01 38 30 1F  0C 19 4E 65  77 20 47 65  |.<...80...New Ge|
6E 65 72 61  74 65 64 20  50 72 69 76  61 74 65 20  |nerated Private |
4B 65 79 03  02 07 80 30  0E 04 04 00  00 00 03 03  |Key....0........|
02 05 20 03  02 05 E0 A1  82 01 03 A2  81 F5 02 01  |.. .............|
02 31 59 A2  57 02 01 04  30 06 04 04  00 00 00 05  |.1Y.W...0.......|
30 1E 06 07  2A 85 03 02  02 0D 01 30  13 06 07 2A  |0...*......0...*|
85 03 02 02  1F 01 04 08  15 B4 3C 18  2B 6E 35 98  |..........<.+n5.|
04 2A 30 28  04 20 74 DA  1E A4 88 11  BA 29 1C 2F  |.*0(. t......)./|
55 FF 4C DD  A2 22 71 27  9F B6 33 8F  AC 06 36 72  |U.L.."q'..3...6r|
A6 63 85 B2  7E 52 04 04  8E 9E 7C 34  30 81 94 06  |.c..~R....|40...|
09 2A 86 48  86 F7 0D 01  07 01 30 1F  06 08 2A 85  |.*.H......0...*.|
03 02 04 03  02 02 30 13  04 08 F9 CC  24 E2 AE 66  |......0.....$..f|
28 49 06 07  2A 85 03 02  02 1F 01 80  66 3A CF E7  |(I..*.......f:..|
58 53 69 E5  49 1A 1D 4C  95 22 E9 43  FF F1 87 DC  |XSi.I..L.".C....|
10 6E A9 BD  34 9D AB 64  34 57 9A 8A  4D 4C D4 C3  |.n..4..d4W..ML..|
9B 8A E1 56  3B 20 D2 6E  B1 7D 99 AC  61 D8 88 C2  |...V; .n.}..a...|
7B 41 63 1B  CE DB 3A 75  AB 8A 6C 5C  5F 1E 9A 2C  |{Ac...:u..l\_..,|
3C 35 41 A7  33 24 47 E2  4D 41 2F 4B  CD 76 08 70  |<5A.3$G.MA/K.v.p|
BF DA 2B 77  F5 6B 6A 8F  FE 35 70 41  60 2E 23 DB  |..+w.kj..5pA`.#.|
6A 4D 62 30  09 06 07 2A  85 03 02 02  23 02 A1 81  |jMb0...*....#...|
92 A0 81 8F  BB 81 8C 30  2D 0C 28 50  75 62 6C 69  |.......0-.(Publi|
63 20 4B 65  79 20 66 6F  72 20 4E 65  77 20 47 65  |c Key for New Ge|
6E 65 72 61  74 65 64 20  50 72 69 76  61 74 65 20  |nerated Private |
4B 65 79 03  01 00 30 0A  04 04 00 00  00 03 03 02  |Key...0.........|
01 02 A1 4F  A0 42 04 40  1E 8B CE FD  7C 95 E8 4F  |...O.B.@....|..O|
11 E3 5A 14  A0 58 FD 5B  CB 3E 24 89  3A DE 91 59  |..Z..X.[.>$.:..Y|
99 EB 27 5B  A3 AF AF 1D  D4 D5 8D 6C  32 A2 64 D3  |..'[.......l2.d.|
8A E6 CD 07  54 0C 76 7B  41 5E 64 54  0B E9 23 02  |....T.v{A^dT..#.|
A7 F4 EA FA  65 CD F6 4B  30 09 06 07  2A 85 03 02  |....e..K0...*...|
02 23 02 A0  82 01 C1 A0  82 01 BD BB  82 01 B9 30  |.#.............0|
19 0C 13 35  31 32 2D 62  69 74 20 70  72 69 76 61  |...512-bit priva|
74 65 20 6B  65 79 03 02  07 80 30 30  04 04 00 00  |te key....00....|
00 04 03 02  05 20 03 02  05 E0 18 0F  32 30 31 33  |..... ......2013|
31 30 32 32  31 32 31 34  33 33 5A 80  0F 32 30 31  |1022121433Z..201|
34 31 30 31  38 32 32 30  30 30 30 5A  A1 82 01 68  |41018220000Z...h|
A2 82 01 57  02 01 02 31  59 A2 57 02  01 04 30 06  |...W...1Y.W...0.|
04 04 00 00  00 05 30 1E  06 07 2A 85  03 02 02 0D  |......0...*.....|
01 30 13 06  07 2A 85 03  02 02 1F 01  04 08 42 59  |.0...*........BY|
7A BF 46 FA  D9 24 04 2A  30 28 04 20  86 FC 00 80  |z.F..$.*0(. ....|
C9 07 31 2D  65 0B C6 93  B8 37 3F FA  C3 BB CF 0C  |..1-e....7?.....|
2A A9 15 C0  9E BF 04 1F  0D F5 B1 ED  04 04 E3 68  |*..............h|
```

```
3C D8 30 81  F6 06 09 2A  86 48 86 F7  0D 01 07 01  |<.0....*.H......|
30 1F 06 08  2A 85 03 02  04 03 02 02  30 13 04 08  |0...*.......0...|
F8 B5 70 EE  E4 BC 82 C4  06 07 2A 85  03 02 02 1F  |..p.......*.....|
01 80 81 C7  48 0C CC 5B  74 8A 44 BC  75 83 22 D2  |....H..[t.D.u.".|
CF 68 AB 1A  9C 74 CC 78  7E 43 88 EB  E8 9C 2D 15  |.h...t.x~C....-.|
C2 CB BC E8  76 35 BA ED  C5 4A EE C5  60 27 3A 30  |....v5...J..`':0|
DC 0A 94 74  90 92 39 B3  88 A5 9C FE  59 44 5F AA  |...t..9.....YD_.|
2B 0F 19 D1  52 CA 71 89  9E D8 6C D9  3E D9 5A FB  |+...R.q...l.>.Z.|
52 E3 67 66  95 23 52 50  D7 D9 10 87  79 1B 1B C2  |R.gf.#RP....y...|
0C 3D BC D9  C9 83 76 4A  D5 D2 F5 34  CF 56 CA 06  |.=....vJ...4.V..|
03 A0 54 5D  AF B1 65 C6  E0 83 75 AB  A0 42 B4 F0  |..T]..e...u..B..|
69 C3 F0 4E  6B 7D 97 37  66 68 DE B9  BC 4E BB E2  |i..Nk}.7fh...N..|
64 20 51 FF  EB 5D 0C 21  72 5B 09 4E  F5 EF C3 7C  |d Q..].!r[.N...||
04 24 DC 11  5C CF FB CC  49 F2 F2 74  4F 82 A7 FC  |.$..\...I..tO...|
49 A5 C4 D4  33 A4 25 2C  AD C7 D3 5E  66 77 D7 14  |I...3.%,...^fw..|
A5 2A 09 F1  41 29 7B DB  30 36 B1 30  0B 06 09 2A  |.*..A){.06.0...*|
85 03 07 01  02 01 02 00  A1 81 F3 A0  81 F0 BB 81  |................|
ED 30 27 0C  22 50 75 62  6C 69 63 20  6B 65 79 20  |.0'."Public key |
66 6F 72 20  35 31 32 2D  62 69 74 20  70 72 69 76  |for 512-bit priv|
61 74 65 20  6B 65 79 03  01 00 30 2C  04 04 00 00  |ate key...0,....|
00 04 03 02  01 02 18 0F  32 30 31 33  31 30 32 32  |........20131022|
31 32 31 34  33 33 5A 80  0F 32 30 31  34 31 30 31  |121433Z..2014101|
38 32 32 30  30 30 30 5A  A1 81 93 A0  81 83 04 81  |8220000Z........|
80 0F EA C5  57 A0 A6 30  EE AC A5 3A  1C CB C9 48  |....W..0...:...H|
6D C1 E1 00  8D CB BA AD  C9 B7 7F 8B  FE 94 32 C1  |m.............2.|
D2 09 DA 85  0D 40 8D 1C  17 21 AC 53  36 34 7E A4  |.....@...!.S64~.|
40 CC 27 A4  9B AD BA 05  58 F5 9D 90  09 2B 4B 39  |@.'.....X....+K9|
1E 0B DF 3C  66 99 EA E9  25 17 13 E1  9E F8 FE AC  |...<f...%.......|
39 3B 26 94  1A 08 BA CC  E7 71 D0 03  24 A0 67 36  |9;&......q..$.g6|
A4 ED 28 7B  21 07 90 32  72 AA 18 38  BA C3 BD 51  |..({!..2r..8...Q|
6B 9C 2A 22  DB EE CA B8  B1 5F 12 DB  1A A1 74 F9  |k.*".....t.|
03 30 0B 06  09 2A 85 03  07 01 02 01  02 00 A7 82  |.0...*..........|
01 20 A0 82  01 1C A1 82  01 18 30 15  0C 0F 54 6F  |. ........0...To|
70 2D 73 65  63 72 65 74  20 44 61 74  61 03 02 06  |p-secret Data...|
C0 30 0D 06  0B 2B 06 01  04 01 E8 00  83 77 01 04  |.0...+.......w..|
A1 81 EF 06  05 29 83 48  BD 52 A2 81  E5 02 01 02  |.....).H.R......|
31 59 A2 57  02 01 04 30  06 04 04 00  00 00 05 30  |1Y.W...0.......0|
1E 06 07 2A  85 03 02 02  0D 01 30 13  06 07 2A 85  |...*......0...*.|
03 02 02 1F  01 04 08 91  50 FE 38 D8  65 B1 49 04  |........P.8.e.I.|
2A 30 28 04  20 4A DE 79  15 31 F1 14  F8 A7 10 E3  |*0(. J.y.1......|
6C 8B 6C 70  12 FE 54 55  FE 93 07 B5  A8 73 7E 28  |l.lp..TU.....s~(|
C3 F4 0B 6C  65 04 04 8C  5D A7 F4 30  81 84 06 09  |...le...]..0....|
2A 86 48 86  F7 0D 01 07  01 30 1F 06  08 2A 85 03  |*.H......0...*..|
02 04 03 02  02 30 13 04  08 56 10 B0  73 50 01 D8  |.....0...V..sP..|
77 06 07 2A  85 03 02 02  1F 01 80 56  B4 A0 8C 8A  |w..*.......V....|
70 75 C6 8B  B1 B0 9D 8B  18 BB A1 A2  E2 2B 3E B0  |pu...........+>.|
B5 BD C6 D6  97 C3 6B 8F  45 46 01 80  23 DB EB 51  |......k.EF..#..Q|
D7 D7 5C 4A  1C CA 6F 37  CD 95 C8 53  2A 10 BA 9B  |..\J..o7...S*...|
EA 09 4D D2  1A 4C C9 49  42 B2 11 2D  7F 1A 19 4D  |..M..L.IB..-...M|
E8 C5 C8 09  55 23 E5 78  28 F6 06 3B  75 3F 8D B3  |....U#.x(..;u?..|
69 6C A7 6B  A0 69 A1 67  30 11 0C 0B  50 75 62 6C  |il.k.i.g0...Publ|
69 63 20 44  61 74 61 03  02 06 40 30  0D 06 0B 2B  |ic Data...@0...+|
06 01 04 01  E8 00 83 77  01 04 A1 43  06 06 29 85  |.......w...C..).|
7D 83 30 01  A0 39 04 37  54 68 69 73  20 69 73 20  |}.0..9.7This is |
73 6F 6D 65  20 6F 70 65  6E 20 64 61  74 61 2E 20  |some open data. |
54 68 65 72  65 27 73 20  6E 6F 20 6E  65 65 64 20  |There's no need |
74 6F 20 65  6E 63 72 79  70 74 20 69  74 2E 00     |to encrypt it.. |
Message digest (hash) of the eContent (ostr header not included):
73 4A 2A AC  3F 43 44 47  BA 37 B3 10  AE 63 93 C1  |sJ*.?CDG.7...c..|
93 90 EC 78  89 DC 66 37  77 DF 16 DA  24 A0 41 63  |...x..f7w...$.Ac|
7B 2F 7B A0  84 A3 93 09  08 D7 2C 07  BC 93 6C 5F  |{/{.......,...l_|
8D CE E7 82  AC 3B B1 57  66 A3 B1 B5  1C 52 F6 3E  |.....;.Wf....R.>|
```

```
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=64 - message digest (see above)

Encoded authAttrs (standalone):
31 6C 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 4F 06  |...*.H.......0O.|
09 2A 86 48  86 F7 0D 01  09 04 31 42  04 40 73 4A  |.*.H......1B.@sJ|
2A AC 3F 43  44 47 BA 37  B3 10 AE 63  93 C1 93 90  |*.?CDG.7...c....|
EC 78 89 DC  66 37 77 DF  16 DA 24 A0  41 63 7B 2F  |.x..f7w...$.Ac{/|
7B A0 84 A3  93 09 08 D7  2C 07 BC 93  6C 5F 8D CE  |{.......,...l_..|
E7 82 AC 3B  B1 57 66 A3  B1 B5 1C 52  F6 3E        |...;.Wf....R.>  |
Calculating HMAC of authAttr:
Key:
CA 0F C3 47  47 09 52 F5  82 06 7D 0A  7A A8 49 08  |...GG.R...}.z.I.|
C7 6D 3C 2F  F8 9C 3B C3  09 31 3B 2A  61 B3 46 F5  |.m</..;..1;*a.F.|
authAttrs HMAC (AuthenticatedData.mac):
26 3C AF B3  0E CB 75 E8  76 EC A3 8B  A3 D2 67 78  |&<....u.v.....gx|
05 06 63 E9  A3 88 67 79  12 AE BA D1  0E 4A 5D 58  |..c...gy.....J]X|
97 7F F3 B8  D7 00 8A 0A  DD 38 AF 0B  38 E4 F2 C3  |.........8..8...|
50 F5 15 A7  6E 75 F4 8A  3B F5 6E F4  CE 23 A9 BA  |P...nu..;.n..#..|
```

Библиография

[1] PKCS #15 — PKCS#15 (версия 1.1) Формат представления информации в криптографическом токене [Cryptographic Token Information Format Standard (v.1.1), RSA Laboratories]

[2] Методические рекомендации ТК 26 — Идентификаторы объектов (OID) технического комитета по стандартизации «Криптографическая защита информации» (ТК 26OID)

[3] Техническая спецификация ТК 26 — Использование алгоритмов ГОСТ Р 34.10 и ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509 (ТК26ИОК)

[4] RFC4357 — В. Попов, И. Курепкин, С. Леонтьев. Дополнительные алгоритмы шифрования для использования с алгоритмами по ГОСТ 28147—89, ГОСТ Р 34.10—94, ГОСТ Р 34.10—2001 и ГОСТ Р 34.11—94 [Popov V., Kurepkin I. and S. Leontiev. 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, Informational, IETF RFC4357, January 2006]

[5] Методические рекомендации ТК 26 — Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147—89 (ТК26УЗ)

[6] RFC5652 — Р. Хаусли. Синтаксис криптографических сообщений [R. Housley. Cryptographic Message Syntax (CMS), Standards Track, IETF RFC5652, September 2009]

[7] RFC4490 — С. Леонтьев, Г. Чудов. Использование алгоритмов ГОСТ 28147—89, ГОСТ Р 34.11—94, ГОСТ Р 34.10—94 и ГОСТ Р 34.10—2001 с синтаксисом криптографических сообщений (CMS) [Leontiev S., Chudov G. 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), Standards Track, IETF RFC4490, May 2006]

[8] Методические рекомендации ТК 26 — Использование алгоритмов ГОСТ 28147—89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS (ТК26CMS)

УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85

Ключевые слова: криптографические протоколы, аутентификация, пароль, ключ, контейнер ключа

Редактор *И.А. Сериков*
Технический редактор *В.Ю. Фотиева*
Корректор *С.В. Смирнова*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 28.11.2016. Подписано в печать 20.12.2016. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,60. Тираж 33 экз. Зак. 3229.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru