RFC 9548
Generating Transport Key Containers (PFX) Using the GOST Algorithms

Abstract
This document specifies how to use "PKCS #12: Personal Information Exchange Syntax v1.1" (RFC 7292) to transport key containers (PFX) for storing keys and certificates in conjunction with the Russian national standard GOST algorithms.

This specification has been developed outside the IETF. The purpose of publication is to facilitate interoperable implementations that wish to support the GOST algorithms. This document does not imply IETF endorsement of the cryptographic algorithms used here.

Status of This Memo
This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9548.

Copyright Notice
Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction 3
2. Conventions Used in This Document 4
3. Basic Terms and Definitions 4
4. PFX 5
   4.1. Structure of PFX 5
   4.2. AuthenticatedSafe 5
      4.2.1. Unencrypted Data 6
      4.2.2. Password-Encrypted Data 6
   4.3. SafeContents and SafeBag 6
5. GOST R 34.10-2012 Key Representation 7
   5.1. Masking GOST R 34.10-2012 Keys 7
   5.2. KeyBag Structure for GOST R 34.10-2012 Key 8
   5.3. OneAsymmetricKey Structure 9
   5.4. EncryptedPrivateKeyInfo Structure for GOST R 34.10-2012 Key 9
6. GOST R 34.10-2012 Certificate Representation 10
7. Security Mechanisms 10
8. Security Considerations 11
9. IANA Considerations 11
10. ASN.1 Modules 12
11. References 12
    11.1. Normative References 12
    11.2. Informative References 13
Appendix A. Examples 13
   A.1. Test Data 13
      A.1.1. Test Certificate 13
1. Introduction

This document provides a specification of the usage of GOST algorithms with PKCS #12 v1.1.

PKCS #12 v1.1 describes a syntax for transfer of personal information such as private keys, certificates, and various secrets.

This memo describes the creation of transport key containers (PFX) for keys and certificates using the GOST R 34.10-2012 algorithm. The GOST R 34.11-2012 algorithm is used to ensure the integrity of PFX.

Caution:

This specification is not a standard and does not have IETF community consensus. It makes use of a cryptographic algorithm that is a national standard for Russia. Neither the IETF nor the IRTF has analyzed that algorithm for suitability for any given application, and it may contain either intended or unintended weaknesses.
2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Basic Terms and Definitions

Throughout this document, the following notations are used:

- **P** a password encoded as a Unicode UTF-8 string
- **S** a random initializing value
- **V** the set of byte strings of length s, where s >= 0; the string b = (b_1,...,b_s) belongs to the set V if b_1,...,b_s belongs to {0,...,255}
- **|A|** the number of components (a length) of the vector A belonging to V (if A is an empty string, then |A| = 0)
- **A || C** a concatenation of two byte strings A, C from V, i.e., a string from V_{|A|+|C|}, where the left substring from V_{|A|} is equal to the string A and the right substring from V_{|C|} is equal to the string C: A = (a_1,...,a_{n_1}) in V_{n_1} and C = (c_1,...,c_{n_2}) in V_{n_2}, res = (a_1,...,a_{n_1},c_1,...,c_{n_2}) in V_{n_1+n_2}
- **F_p** a finite prime field represented as a set of q integers {0,1,...,q-1}, where q > 3 - prime number
- **b mod q** the minimum non-negative number comparable to b modulo p
- **INT(b)** integer INT(b) = b_1 + b_2 * 256 +...+ b_s * 256^{s-1}, where b belongs to V

This document uses the following terms and abbreviations:

- **Signature** one or more data elements resulting from the signature process (Clause 3.12 of [ISO14888-1]). Note: The terms “digital signature”, “electronic signature”, and “electronic digital signature” are considered equivalent in this document.
- **Signature key** set of private data elements specific to an entity and usable only by this entity in the signature process (Clause 3.13 of [ISO14888-1]). Note: Sometimes called a private key.
- **Verification key** set of public data elements that is mathematically related to an entity’s signature key and is used by the verifier in the verification process (Clause 3.16 of [ISO14888-1]). Note: Sometimes called a public key.
4. PFX

The PFX (see [RFC7292]) is designed for secure storage and data transfer. The scope of this document is to define how PFX is used for private key and certificate protection with a password when GOST R 34.10-2012 is applied.

4.1. Structure of PFX

In accordance with [RFC7292], PFX has the following structure:

```
PFX ::= SEQUENCE
{  version     INTEGER {v3(3)}(v3,...),
    authSafe    ContentInfo,
    macData     MacData OPTIONAL
}
```

The fields of the PFX have the following meanings:

- version is the syntax version number; the only allowed value for this specification is 3.
- authSafe contains the data of type ContentInfo. In the case of password integrity mode, the authSafe.content field has a Data type value and contains a BER-encoded value of the AuthenticatedSafe structure.
- macData has a MacData type; in the case of password integrity mode, the macData field should contain information about the algorithm and parameters for password key generation. Integrity control is ensured by using the HMAC_GOSTR3411_2012_512 algorithm: the macData.mac.digestAlgorithm.algorithm field contains the HMAC_GOSTR3411_2012_512 algorithm identifier (see Section 7). When processing PFX, this field should be checked first.

4.2. AuthenticatedSafe

The AuthenticatedSafe structure is a sequence of ContentInfo values (see [RFC5652]):

```
AuthenticatedSafe ::= SEQUENCE OF ContentInfo
   -- Data if unencrypted
   -- EncryptedData if password-encrypted
   -- EnvelopedData if public key-encrypted
```
4.2.1. Unencrypted Data

If the data is not encrypted, then the content field is the BER-encoded value of the SafeContents structure. The contentType field is set to the id-data type.

4.2.2. Password-Encrypted Data

When password integrity mode is used, the data is represented as an EncryptedData structure (see [RFC5652]). The encryption algorithm and parameters have the following values:

```
ContentEncryptionAlgorithmIdentifier ::= SEQUENCE
{  
  encryptionAlgorithmOID   OBJECT IDENTIFIER,
  parameters              PBES2-params
}
```

The PBES2-params type is defined in [RFC9337]. The content should be encrypted according to the encryption algorithm in the PBES2 scheme, as described in [RFC9337]. The following identifier MUST be specified in the EncryptedData.EncryptedContentInfo.contentEncryptionAlgorithm.encryptionAlgorithmOID field:

```
{  
  iso(1) member-body(2) us(840) rsadsi(113549)
  pkcs(1) pkcs-5(5) pbes2(13)
}
```

The encrypted content is specified in the EncryptedData.EncryptedContentInfo.encryptedContent field.

4.3. SafeContents and SafeBag

In accordance with [RFC7292], the SafeContents structure is a sequence of SafeBag:

```
SafeContents ::= SEQUENCE OF SafeBag
```

where

```
SafeBag ::= SEQUENCE
{  
  bagId         BAG-TYPE.&id ({PKCS12BagSet})
  bagValue [0]  EXPLICIT BAG-TYPE.&Type({PKCS12BagSet}@bagId)
  bagAttributes SET OF PKCS12Attribute OPTIONAL
}
```
The fields of SafeBag have the following meanings:

- bagId is an object identifier; it defines the type of object.
- bagValue is the value of an object.
- bagAttributes contains the users' names, the key identifiers, and other additional information. This field is optional.

See [RFC7292], Section 4.2 for the different bag types. This document describes the two object types of the SafeBag structure:

1. pkcs8ShroudedKeyBag
2. certBag

When password integrity mode is used, the private key has the following structure:

```
pkcs8ShroudedKeyBag  BAG-TYPE ::= 
{                       
  PKCS8ShroudedKeyBag IDENTIFIED BY {bagtypes 2} 
}
```

The bagValue field contains the key and information about the key, in encrypted form, in the EncryptedPrivateKeyInfo structure.

A certBag contains a certificate of a certain type. Object identifiers are used to distinguish between different certificate types.

```
certBag  BAG-TYPE ::= 
{         
  CertBag IDENTIFIED BY { bagtypes 3 } 
}
```

If the certificate is not encrypted, the CertBag structure is placed in the Data structure (see [RFC5652]). If the certificate is encrypted, the CertBag structure is placed in the EncryptedData structure (see [RFC5652]).

## 5. GOST R 34.10-2012 Key Representation

This section describes the GOST R 34.10-2012 private key representation for asymmetric key pairs. Masked keys should be used to ensure that private keys are protected from leaking through side channels when reading and performing operations with keys.

### 5.1. Masking GOST R 34.10-2012 Keys

The masking algorithm is defined by the basic cryptographic transformation operation of the algorithm: multiplication in the $F_q$ field for GOST R 34.10-2012 keys.
Let $M_1, M_2, ..., M_k$ be a sequence of $k$ masks. Let $M_i()$ denote the operation of applying the $i$-th mask and $M_i^{-1}()$ denote the operation of removing the $i$-th mask, $1 \leq i \leq k$. Let $K$ be a key. The masked key $K_M$ is obtained by applying the masking operation $k$ times:

$$K_M = M_k(...(M_2(M_1(K))...).$$

Unmasking is performed by applying the removal operation $k$ times, but in reverse order:

$$K = M_1^{-1}(...(M_{k-1}^{-1}(M_k^{-1}(K_M))...).$$

The masked key is represented as the sequence

$$I = K_M || M_1 || M_2 || ... || M_k.$$

Let the key $K$ be $n$ bits in length; then, the sequence $I$ is represented in memory as a sequence of $(k + 1)*n$ bits. $I$ is represented in little-endian format. It is possible to use an unmasked private key (i.e., $k = 0$, $K_M = K$). For GOST R 34.10-2012 keys, the masking operation is the multiplication of the key by the inverse of the mask: $\text{INT}(K_M) = \text{INT}(K) \cdot \text{INT}(M)^{-1} \mod Q$, where the $Q$ value is taken from the key parameters. The operation of removing the mask is the multiplication of the masked key by the mask: $\text{INT}(K) = \text{INT}(K_M) \cdot \text{INT}(M) \mod Q$. The public key is specified by a pair of coordinates $(x, y)$ as defined in GOST R 34.10-2012, presented in the following format:

- a public key corresponding to the GOST R 34.10-2012 algorithm with a key length of 256 bits has the GostR3410-2012-256-PublicKey representation. It is specified by a 64-byte string, where the first 32 bytes contain the little-endian representation of the $x$ coordinate and the last 32 bytes contain the little-endian representation of the $y$ coordinate.
- a public key corresponding to the GOST R 34.10-2012 algorithm with a key length of 512 bits has the GostR3410-2012-512-PublicKey representation. It is specified by a 128-byte string, where the first 64 bytes contain the little-endian representation of the $x$ coordinate and the last 64 bytes contain the little-endian representation of the $y$ coordinate.

The public keys GostR3410-2012-256-PublicKey and GostR3410-2012-512-PublicKey MUST be DER encoded as an octet string in accordance with Section 4.3 of [RFC9215]:

```
GostR3410-2012-256-PublicKey ::= OCTET STRING (64),
GostR3410-2012-512-PublicKey ::= OCTET STRING (128).
```

### 5.2. KeyBag Structure for GOST R 34.10-2012 Key

In accordance with [RFC7292], a KeyBag is defined as information about a private key represented as the PrivateKeyInfo structure:
In accordance with [RFC5958], information about a private key is presented in the following form:

```
PrivateKeyInfo ::= OneAsymmetricKey
```

### 5.3. OneAsymmetricKey Structure

In accordance with [RFC5958], OneAsymmetricKey has the following structure:

```
OneAsymmetricKey ::= SEQUENCE
{  
  version                 Version,  
  privateKeyAlgorithm     PrivateKeyAlgorithmIdentifier,  
  privateKey              PrivateKey,  
  attributes              [0] Attributes OPTIONAL,  
  ...  
  [1] publicKey           [1] PublicKey OPTIONAL],  
  ...  
}
```

The fields have the following meanings:

- version identifies the version of OneAsymmetricKey. If publicKey is present, then version is set to 2; else, version is set to 1.
- privateKeyAlgorithm identifies the private key algorithm and optionally contains parameters associated with the asymmetric key pair. For GOST R 34.10-2012 private keys, the identifiers of the corresponding public keys are used; they are defined in [RFC9215]. The use of identifiers and public key parameters is defined in [RFC9215].
- privateKey is an OCTET STRING that contains the value of the masked private key I.
- attributes are optional. They contain information corresponding to the public key (e.g., certificates).
- publicKey contains the value of the public key GostR3410-2012-256-PublicKey or GostR3410-2012-512-PublicKey encoded in a BIT STRING. This field is optional.

### 5.4. EncryptedPrivateKeyInfo Structure for GOST R 34.10-2012 Key

In accordance with [RFC7292], the encrypted information regarding the private key is defined as the PKCS8ShroudedKeyBag structure:
In accordance with [RFC5958], EncryptedPrivateKeyInfo has the following structure:

```
PKCS8ShroudedKeyBag ::= EncryptedPrivateKeyInfo

In accordance with [RFC5958], EncryptedPrivateKeyInfo has the following structure:

EncryptedPrivateKeyInfo ::= SEQUENCE
{  
  encryptionAlgorithm EncryptionAlgorithmIdentifier,
  encryptedData       EncryptedData
}

EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
EncryptedData ::= OCTET STRING
```

The fields have the following meanings:

- `encryptionAlgorithm` identifies the algorithm under which the private key information is encrypted. Encryption **MUST** use the PBES2 scheme. The algorithm and parameters of this scheme are presented in [RFC9337].
- `encryptedData` is the DER-encoded PrivateKeyInfo structure.

6. **GOST R 34.10-2012 Certificate Representation**

In accordance with [RFC7292], a CertBag is defined as information about a certificate and has the following structure:

```
CertBag ::= SEQUENCE
{  
  certId                  BAG-TYPE.&id ({CertTypes}),
  certValue [0] EXPLICIT  BAG-TYPE.&Type ({CertTypes}{@certId})
}
```

The fields have the following meanings:

- `certId` identifies the type of certificate.
- `certValue` contains the certificate.

7. **Security Mechanisms**

Let the sender and receiver have a previously agreed-upon password P. The sender generates a password key using the PBKDF2 algorithm in accordance with [RFC9337] and uses it to encrypt the transmitted private key. The recipient independently generates a password key using the same PBKDF2 diversification algorithm in accordance with [RFC9337] and uses it to extract the private key from the PFX.
The same password P is used to encrypt different sections of the PFX using a different random initializing value S with a length of 8 to 32 bytes, where S and P are the input parameters of the PBKDF2 function. The password MUST be encoded as a Unicode UTF-8 string and fed into the PBKDF2 algorithm as a P parameter.

The integrity of the PFX is ensured by using the HMAC_GOSTR3411_2012_512 algorithm in accordance with [RFC7836]. To check the integrity of the PFX with the HMAC_GOSTR3411_2012_512 algorithm, the key for this algorithm is also generated by using the PBKDF2 algorithm in accordance with [RFC9337], with the same value for the P parameter and a different initializing value S with a length of 8 to 32 bytes. The dkLen parameter for the PBKDF2 algorithm is set to 96 bytes. The key for the HMAC_GOSTR3411_2012_512 algorithm must be the last 32 bytes of the 96-byte sequence generated by the PBKDF2 algorithm. The PBKDF2 algorithm parameters S and c are saved in the macData.Salt and macData.iterations fields, respectively. The HMAC_GOSTR3411_2012_512 function is calculated from the content field of the authSafe structure field. The authSafe structure field is a PFX structure field. The value of the calculated checksum is saved in the macData.mac.digest field. The macData.mac.digestAlgorithm.algorithm field contains the following algorithm identifier:

```
  id-tc26-gost3411-12-512 ::= {
    iso(1) member-body(2) ru(643) rosstandart(7) tc26(1)
    algorithms(1) digest(2) gost3411-12-512(3)
  }
```

The macData.mac.digestAlgorithm.parameters field isn't used and should be omitted.

8. Security Considerations

The masked keys SHOULD be used to ensure that private keys are protected from leaking through side channels when reading and performing operations with keys. Applications MUST use unique values for ukm and S in the PBKDF2 algorithm. It is RECOMMENDED that parameter S consist of at least 32 octets of pseudorandom data in order to reduce the probability of collisions of keys generated from the same password. The password MUST be encoded as a Unicode UTF-8 string and fed into the PBKDF2 algorithm as a P parameter. For more information, see [RFC9337]. Encryption MUST use the PBES2 scheme to encrypt private keys. Public keys MUST be DER encoded as an octet string in accordance with [RFC9215]. Passwords SHOULD be stored in a secure way. For information on security considerations for generating PFX, see [RFC7292].

9. IANA Considerations

This document has no IANA actions.
11. References

11.1. Normative References


11.2. Informative References


Appendix A. Examples

This section contains examples of using GOST cryptographic algorithms to create a PFX.

A.1. Test Data

In all examples, the following data is used.

A.1.1. Test Certificate

This section contains a test certificate in BASE64 format.
A.1.2. Test Key

This section contains test key bytes in hexadecimal.

F95A5D44C5245F63F2E7DF8E782C1924EADCB8D06C52D91023179786154CBDB1
561B4DF759D69F67EE1FB5B68800E134BA12818DA4F3AC75B6E6F9256911

A.2. Example of a PFX with a Password-Protected Key and Unencrypted Certificate

In this example, the PKCS8ShroudedKeybag structure is used to store the key, which is placed in the Data structure. The certBag structure is used to store the certificate, which is placed in the Data structure. The following password is used to encrypt the key and provide integrity control: "Пароль для PFX". The password is in hexadecimal:

D09FD0B0D180D0BED0BBD18C2D00B4D0BBBD18F20504658

The key encryption algorithm identifier:

1.2.643.7.1.1.5.2.2
A.2.1. PFX in BASE64 Format

```
MIIFKwIBAzCCBMQGCSqGSIb3DQEHAaCBLUEggSxMIIeTCCAswGCsGSIb3DQEHE
AaCCAr8Egg5MIIctTCCArE6Cyq0GSIb3DQEMCgDoIICSjCAK2YGCiq0GSIb3DQEm
FgGgGg2BIIcMjCA4wHhbOAMCAQICBAMwMDAwMFowMDQtQSMiIzMTAwMDAwMFowO
A1UECHMEVesyNjEnMCUGAUEmA0EgVesyNjogR9TVCazNC4xMCMxMaYNTyt
Ym10MB4XRDAxMDwMDAwMFowMDQwaDQwMDEtQSMiIzMTAwMDAwMFowO
A1UECHMEVesyNjEnMCUGAUEmA0EgVesyNjogR9TVCazNC4xMCMxMaYNTyt
Ym10MB4XRDAxMDwMDAwMFowMDQwaDQwMDEtQSMiIzMTAwMDAwMFowO
MIGeMBGcCgFwAQCMECMA4GCsGfwACgAECQ0BhAAGeYc0I7davCdOGVcYqFQ
I2fUIOzR0ByYRIeOtc1TRpare/6sRvRapqzz0+K21LDbYYfDPs2Sqa13Zm+Ts
/JULv59qOBF2cYPfYB/0kA4+K79yvz7r8+4WE8emZf8T3ae/J106xGunecH1/G4
hMts9HLYnx bwDMVNeuIvH6gqz08hczBdBJhBjgVHSMDXDBagBSSbA5MRGaiQbip
iunw7JWbzy6RFKqeg8pDowODENASGA1UECMEVesyNjEnMCUGAUEmA0EqVesy
NjogR9TVCazNC4xMCMxMaYNTytYm10bgOBbQMB8GA1UdDgQWBBR+BlCmJAYm
awioV+55AF6ydegdDAKggqHMQAOEDAgNBAaepqfHQQ6yvR5Pt50MD1NFI1idey
K5a0q6f5qBe2czLlF1A9Q8M9ya658X153lZlgQ0XVCFQysg4DFOBrphHyBAvVDAj
BgzkhJ1i9w8BCFRUXFg0ueVv0+dS25MlCIChpmGc/8A0uwEwLQYJKoIZhNACqKU
MSSAeHgwADEAMgBGAlHAaaQ81AG4AZAsAhkATgBhAG0AZTCCadGCSqGSIb3DQEH
AaCCaCecggHGMIIwjjCCAc4BCyqGSIb3DQEMCgEcII8VzCCAVMwWQYJKoIZhNv
AQUNMEmwKQJKozhNACvNAqNNMwBECFkn47NwmuqagAIAADAMBggqHMAQEOoAgUA
MB8G8CGsFawcbBAQCAjaSBBAAlmt2WDfaPj1sAs0mLkgzBHIHDmVaeobbrWNVDSnX
JLWygYrlOipQDA/2HEnBZ34uFOLheUqkiKPCoPfbR2GB1YYTVK9lbczgcaca
EQYziDXteSBOC2OxpkWf6eA1bdJLC/SqPurPyyKiOMVRUROPohibsFASD138HDHlD
0dL5f6q4a4PWLrWbQweUFOOyP4dolTb37AOw1ejbbyRQhh4WxiA0xRQAh
qo4hn4QGVY92/HfVjuT3CndQdMWh8/e1h1RHLNfRXN91fZc231a201yPzP1U
yLrU1TClbHr1nIrrppPDMlFNMt9dJ7KGC01i7Zm5nHQChbyx1XwcfYxVDAjbBqk
hrk39gw8BCFRUXFg0ueVv0+dS25MlCIChpmGc/8A0uwEwLQYJKoIZhNACqKUMSae
HgwADEAMgBGAlHAaaQ81AG4AZAsAhkATgBhAG0AZTCEwCqYIKoUBdwBBAgME
QAbkKwu4hn7PsIYIEhu0bctVPzJi3W9LvCkUv0scB9G6E9KFE0Tn0bGJSGK5J1U
Kko0sXbA7+BVZf3hCVVQh9UICEVt0+VpuskAgIIA==
```
SEQUENCE:
  CONTEXT SPECIFIC (0):
    INTEGER:2
  INTEGER:26000004
  SEQUENCE:
    OBJECT IDENTIFIER:
      [1.2.643.7.1.1.3.2]
  SEQUENCE:
  SET:
    OBJECT IDENTIFIER:
      organizationName [2.5.4.10]
    PRINTABLE STRING:'TK26'
  SET:
    OBJECT IDENTIFIER:commonName
      [2.5.4.3]
    PRINTABLE STRING:
      'CA TK26: GOST 34.10-12 256-bit'
  UTC TIME:'010101000000Z'
  UTC TIME:'491231000000Z'
  SEQUENCE:
  SET:
    OBJECT IDENTIFIER:
      organizationName [2.5.4.10]
    PRINTABLE STRING:'TK26'
  SET:
    OBJECT IDENTIFIER:commonName
      [2.5.4.3]
    PRINTABLE STRING:
      'ORIGINATOR:
        GOST 34.10-12 512-bit'
  SEQUENCE:
  OBJECT IDENTIFIER:
    [1.2.643.7.1.1.1.2]
  SEQUENCE:
    OBJECT IDENTIFIER:
      [1.2.643.7.1.1.2.1]
  OCTET STRING UnusedBits:0:
    B48BB75ABC290E18655C62A
    14FB52D5F50B444EC1D1F68
    04487B4B5C9534664AB7BFA
    B346E5516A9AB3CCEF8AD8B5
    2C3A5B55F0CB364AA6B5DD
    937E4EFC9525BF9F6A0850
    76718A45C81FFG921E32BB
    F72BF3EEBF3EE1613412665
    FF13DA7BF275268EB11AE9
    DE707DF1B884CB6CF476B0
    F916F02433DB5468B81D5EA0CE
SEQUENCE:
  OBJECT IDENTIFIER: authorityKeyIdentifier
  [2.5.29.35]

OBJECT IDENTIFIER: subjectKeyIdentifier
  [2.5.29.14]

OBJECT IDENTIFIER: commonName
  [2.5.4.3]

OBJECT IDENTIFIER: organizationName
  [2.5.4.10]

PRINTABLE STRING: 'TK26'

OBJECT IDENTIFIER: friendlyName
  [1.2.840.113549.1.9.20]

BMP STRING: 'p12FriendlyName'

OBJECT IDENTIFIER: localKeyID
  [1.2.840.113549.1.9.21]
SEQUENCE:
  OBJECT IDENTIFIER:data [1.2.840.113549.1.7.1]
  CONTEXT SPECIFIC (0):
  OCTET STRING:
    SEQUENCE:
      OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
      CONTEXT SPECIFIC (0):
        OCTET STRING:
          SEQUENCE:
            SEQUENCE:
              OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
              CONTEXT SPECIFIC (0):
                OCTET STRING:
                  SEQUENCE:
                    SEQUENCE:
                      OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                      CONTEXT SPECIFIC (0):
                        OCTET STRING:
                          SEQUENCE:
                            OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                            CONTEXT SPECIFIC (0):
                              OCTET STRING:
                                SEQUENCE:
                                  OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                  CONTEXT SPECIFIC (0):
                                    OCTET STRING:
                                      SEQUENCE:
                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                        CONTEXT SPECIFIC (0):
                                          OCTET STRING:
                                            SEQUENCE:
                                              OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                              CONTEXT SPECIFIC (0):
                                                OCTET STRING:
                                                  SEQUENCE:
                                                    OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                    CONTEXT SPECIFIC (0):
                                                      OCTET STRING:
                                                        SEQUENCE:
                                                          OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                          CONTEXT SPECIFIC (0):
                                                            OCTET STRING:
                                                              SEQUENCE:
                                                                OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                CONTEXT SPECIFIC (0):
                                                                  OCTET STRING:
                                                                    SEQUENCE:
                                                                      OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                      CONTEXT SPECIFIC (0):
                                                                        OCTET STRING:
                                                                          SEQUENCE:
                                                                            OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                            CONTEXT SPECIFIC (0):
                                                                              OCTET STRING:
                                                                                SEQUENCE:
                                                                                  OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                  CONTEXT SPECIFIC (0):
                                                                                    OCTET STRING:
                                                                                      SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SEQUENCE:
                                                                                        OBJECT IDENTIFIER:
pkcs-12-pkcs-8ShroudedKeyBag
                                                                                        CONTEXT SPECIFIC (0):
                                                                                          OCTET STRING:
                                                                                       SET:
                                                                                     OBJECT IDENTIFIER:localKeyID
                                                                                          [1.2.840.113549.1.9.21]
                                                                                      SET:
                                                                                           OCTET STRING:
                                                                                          795574F9D4B6E4C20224
                                                                                           286998673FF0A14C04D
                                                                                      SET:
                                                                                           OCTET STRING:
                                                                                            friendlyName

A.2.3. Decrypted Key Value in BASE64 Format

MIHiAgEBMBcGCCqFAwcbAQECMAAsGCSqFAwcBAgECAQRAEWkl+eblsHWs86SNgRkqSxM0qGhvbR/uz5/WWfdNGlaxUwVhpcXixDUzmQzWnzgBkse17f5/JjxyTRF1a+YGbgQOQ07davCkOGGCvQyFpS1fuIy0zB0fyYAR1e6tc1TRpare/qzRuVRapqzz0+kZ1LdpYVFpDSZsa13ZNV+Ts/JjUl59qCFB2ycPfYB/6kh4+k79yy7r8+4WE0EmZf8T3ae/J1Jo6xGunechH1/G4hMts9HYLnxbwJDMNNGuIHV6gzc=

A.2.4. Decrypted Key Value in ASN.1 Format

0 226:SEQUENCE:
  3 1: INTEGER: 1
  6 23: SEQUENCE:
    8 8: OBJECT IDENTIFIER: [1.2.643.7.1.1.1.2]
    18 11: SEQUENCE:
      20 9: OBJECT IDENTIFIER: [1.2.643.7.1.2.1.2.1]
    31 64: OCTET STRING:
      116925F9E6E5B075ACF3A48D8112AA4B138EB06585BBD1FEE679FD6
      59F74D1B56BD4C158697172310D9526CD08DCE2A4192C788EDF
      E7F2635F245445D5AF9
  97 129: CONTEXT SPECIFIC (1):
    01B4BBB75ABC290E18655C62A14FB52D5F50844ECC1D1F6004487B
    4B5C9534696A7BFBAB346E5516A9AB3CCEF8ADB52CA35855F0CBF3
    64A4A6B5D937E4ECCFC952BF96A805076718A45C81FF4921E3EB2
    BF72BF3EEBF3EE1613412665FF13DDA7BF27526EB11AE9DE707D
    F1BB84CB6CF4760B9F16F024330D546B881D5E8CE

A.3. Example of a PFX with a Password-Protected Key and a Password-Protected Certificate

In this example, the PKCS8SHroudedKeybag structure is used to store the key, which is placed in the Data structure (see [RFC5652]). The certBag structure is used to store the certificate, which is placed in the EncryptedData structure (see [RFC5652]). The following password is used to encrypt the key and provide integrity control. The password is in hexadecimal.
The key encryption algorithm identifier:

1.2.643.7.1.1.5.1.1

The certificate encryption algorithm identifier:

1.2.643.7.1.1.5.1.2

A.3.1. PFX in BASE64 Format

```
MIIFjAIBAzCCBBSUfGcgsGSIb3DQHEAcCBRYEggsUSMIIFdJCcA0EGQsGSIb3DQEH
BgCCAzIwgMuAgEAMIID.JvWyJKoZKhvNAQcmBOMGQsGSIb3DQFDTIBMCKGQsG
SIb3DQFDTIBAaAgPuSVsSwGJQICCAAwD1YkOUDwEBBIAFADAbBkgkqQMAHEOG
AQWdQgM9Hk3dagtS4cG+/x+gIIcCWgPqxxN+SrKbruRf95Yaf5At01frgMn
fIEULfzmTg/Bde5IQQ+Vbnri3vkdsmpr6iz2+e4W+i+ndeEC86W6A6X/G22z/
RAH2d
YRvm6cCWwW+YrQz4+8/RQL/9huamD5hMLPvLsYrEa1OowbgXayDSwARVJLQYq
sLNMzK5VlN+friS5wszJ3AtVgB8EuP41a4EwKPy2g3mH4S6WmmQRC6W7aoqmIiFF
PJEJNn5KZMJ6jZS6s6FfYNNXRMNQntv3r1oy6eAaaLY6A6jsekmopodHmOjv
Y4eEoEs0xhpxXz69PXT+2eBHV6ShesBhxQxAd1DqPtTafMjNK8rqKCap9TTPg
vONvO5w9dwegqzRQzjum8dzv4mW9aQw7T8/UcXDrWRz3k6ijFpLaA9+8ZMTEO
RHHbRbVw6L0Y/WNvXpxgWfGyuPxyS13yNdZIpmBee51U/X7VkzjFsUMG3F8fYR61k
4/QnpK11QvU714YKfKuOqzsnhZG1vL1NGID62p1+J13vuuw1m2DMRmkugM9QF9U9v
/kRP+c2uBHdUTGEGUSNhF0p87+w3Vxp1atGWXH9fmISPBdK2f3wn+/rwoqEuiJM
i/BaCv1U/MBDMtKhAoc9j31UY5sd14fsrWYDJM/jq/8P9n6tuo+ocPbq3V3uwPM/8
L4x4qThtYw++/+fPG0/P6xadNEiEII/TYjenLvFXjAHOVJVsVeCu/t3EsMYQddNCh
rFk/Ic2PdIOYkU4/benW0qrKegSybNZuF1WI4z1mIB8L9dTTB0hky45yQX1ID8D
k1ErYdtedEpzt/4zuPbIwmmCEIOouUxUtGuJP+tcpXwEXRMKw2Ubi3qBJpn7DUM8
trsRM9p0dd18mT/Yfh9+B8d7ZBvXqU70IMPEGexbUKHyFCCny19J8V92StbIz
Elxla1VebjCCAcUGSGsGSIb3DQHEAgCAAcBryEGgyMIIbrJCAaoGCyqGSIb3DQEM
CgEcOIlIgBZQzCCAT8wVOJXkoZIhvNAQUNMEGwKQYJKoZIhvNAQUNMMEBwCPE8Qk80
1twvAgLIADABMBggqgQMQHAAEQeanUAM9BcGQsfAawCBAAQTATBOA9wzxSqq9AAAAA
AAAEeGwUq93m3Rdzk5mdE6EYw7s7ZkX5AnrZwuhPsqDjAzgn761ExJ+wwu1Ns
9PcHF1WUvXjY/10qJ9Xppr9UoP4604ICXp1hcy8dGk/MzIvHRVC63K2nTwq4kKT
kgX9lHFLzdn16dhq1X0+d9q98G8P8EYXBCIBYxLMl1Arcc97KVstJU3mNfrr7E7qu
Tr80ATSOtsq50zpFyprznVPVPCdO1dijpymZxNdvyw8BzqTtrRvDXCYATOGzezPwH
C13MLW9HdJlJlMB2GhbKQyW6uj1lTJs0+WNdX/AT2FL1L1FSS3c1j9M9VQWvYj
KoZIhvNAQKNVWYEF1H1vDnpTuUTaC1QoaZnHP/PAKFMNBM0CGCSQGSIb3DQEFJDeG
Hh4Ac2AaADIArAgQGyAGKAZQ8BUAGQAB5A4E4AQ8tAGUwXjBOA0GCQFAwCBADID
BETDpka2JmXdnvR03x99yQzUqJ8P8exeOpl7m2DZqtFJe5zquW1uk/7V0cfv5r2
bKmBnsL0s2rPT8hBOoeAZvO0BIAjGIHUw6IjQ2QCCCAAC
```

A.3.2. PFX in ASN.1 Format

```
0 1420:SEQUENCE:
  4 1:  INTEGER:3
  7 1317:  SEQUENCE:
    11 9:   OBJECT IDENTIFIER:data [1.2.840.113549.1.7.1]
  22 1302:   CONTEXT SPECIFIC (0):
```

Karelina Informational Page 20
26 1298:  OCTET STRING:
30 1294:   SEQUENCE:
34  833:     SEQUENCE:
38    9:      OBJECT IDENTIFIER:
:        encryptedData [1.2.840.113549.1.7.6]
49  818:     CONTEXT SPECIFIC (0):
53  814:      SEQUENCE:
57    1:        INTEGER:0
60  807:      SEQUENCE:
64    9:        OBJECT IDENTIFIER:
:          data [1.2.840.113549.1.7.1]
75    85:      SEQUENCE:
77    9:        OBJECT IDENTIFIER:[1.2.840.113549.1.5.13]
88   72:      SEQUENCE:
90    9:       OBJECT IDENTIFIER:
[1.2.840.113549.1.5.12]
103  28:      SEQUENCE:
105    8:        OCTET STRING:'14B92546B12C068D'
115   12:        SEQUENCE:
119    8:         OBJECT IDENTIFIER:
[1.2.643.7.1.1.4.2]
131    0:         NULL:
133  27:       SEQUENCE:
135    9:      OBJECT IDENTIFIER:[1.2.643.7.1.1.5.1.2]
146  14:      SEQUENCE:
148   12:        OCTET STRING:
:            F4793775A82D4B8F3E1BFC7E
162  705:      CONTEXT SPECIFIC (0):
```
:  AEFEDDC4B0C60741D74D0A1AC593F21CD8F
:  74840EC81E3F7A7A562DA6AC7A049BC9936
:  E175588E3397988F3D2FC753401524872E
:  39C905D99430FC93512B61DB5D123EDCFF
:  E33B92A589E6C021084683AE497B46BB93F
:  EB5B71174A3356B1822DEA63A67ECE35
:  35F0C86CAD133DA4375A765F264FF5F87D
:  F81FD0D4355C6042EEF494C3419EC5B52
:  4607B850829F28BD27457DD92B5B233125C
:  656B555E6E

871  453:   SEQUENCE:
875    9:    OBJECT IDENTIFIER: data [1.2.840.113549.1.7.1]
886  438:    CONTEXT SPECIFIC (0):
890  434:      OCTET STRING:
894  430:       SEQUENCE:
898  426:         SEQUENCE:
902    11:          OBJECT IDENTIFIER:
906:          pkcs-12-pkcs-8ShroudedKeyBag
915  323:          CONTEXT SPECIFIC (0):
919  319:           SEQUENCE:
923    85:             SEQUENCE:
925     9:              OBJECT IDENTIFIER:
936    72:               SEQUENCE:
938    41:                SEQUENCE:
940     9:                 OBJECT IDENTIFIER:
951    28:                  SEQUENCE:
953     8:                    OCTET STRING:
963     2:                      INTEGER: 2048
967    12:                       SEQUENCE:
969     8:                         OBJECT IDENTIFIER:
979     0:                          NULL:
981    27:                       SEQUENCE:
983     9:                         OBJECT IDENTIFIER:
994    14:                          SEQUENCE:
996    12:                            OCTET STRING:
1010   229:                                OCTET STRING:
2A8FD9B8DD10DF2B984C77411E630B3B
7EB64AFF900DA6C1484FE6A9C38C066
09FB8A513127EC2EB59D2F4F0A17D65
6EB2F765FFD5C981B0BEF0D80AE293A1
EB8097A65721732D1DA4FCCCC8B4745
50B9C0ADA74F1C10E24293967F1784B1
73A03D7A761B6A5FF4FB75083D1BCA44
E44CCB086115C8B502B373F64ECA56
C49B8D32316BFAF1B0B1A4EBF340134
903ADB2AE74CE9172AE9CE754F182ACE
74B89E9CA667135DB80F3C6D9C648E45
56F1B9B813386AB3D29C070A55942C70
FD2C86A32CC8761A104AC9C83A82325
96D26C613F9635D5FF013D852E2D4B15
24B7F828FD
```
### A.3.3. Decrypted Key Value in BASE64 Format

```
MIHiAgEBMBcGCCqFAwcBAQECCMAgsGCSqFBwcBAgECACAQRAEwlkl+eblsHw86SNgRKq
SxMOgGhvrRuZ5/WWfdNG1axvVwVhpcXIxDZUzQuNzqJBkseI7f5/JJxYTFRF1a
+Y9BgQG0l7davCkOGGVCgYqPstS1fuROzB0yYARIe8tc1TRpare/qzRvVRapqzzO
+K2LdpYYfDPS2Sqa13ZNI+Ts/JUIv59qCFB2cYpFyB/8kh4+K79yv7zr8+4WE0Em
Zf8T3ae/J1Jo6xGunechH1/G4hMts9HYLnxbwJDMNVGuIHV6g zg==
```

### A.3.4. Decrypted Key Value in ASN.1 Format

```
0 226:SEQUENCE:
  3 1: INTEGER: 1
  6 23:SEQUENCE:
  8 8: OBJECT IDENTIFIER: [1.2.643.7.1.1.1.2]
  18 11:SEQUENCE:
  20 9: OBJECT IDENTIFIER: [1.2.643.7.1.2.1.2.1]
  31 64:OCTET STRING:
    116925F9E6E5B075ACF3A48D8112AA4B130E80685BD1FEE679FD6
    59F74D1B56B1BD4C158697172318D9526CD0B8DCE2A192C788EDF
    E7F2635F24C5445D5AF9
  97 129:CONTEXT SPECIFIC (1):
    01B488B75AC2B299E18556C2A14F5B2D5F50844EC1D1F6804487B
    4B5C9534696AB7FBAB346E5516A9AB3CCEF8ADB52C3A585580CFB3
    64A4A685D9273E4ECFC952BF96A85076718A45C81FF4921E3E2B
    BF72BF3EEBF3EE1613412665FF13DAA7BF27526EB11AE9DE707D7
    F1B884C6BF4760B9F16F024330D546B881D5EA0CE
```
Acknowledgments

The author thanks Potashnikov Alexander, Pianov Semen, and Smyslov Valery for their careful readings and useful comments, and Chelpanov Alexander for his help with the registration of identifiers.

Author's Address

Ekaterina Karelina (EDITOR)
InfoTeCS
2B stroenie 1, ul. Otradnaya
Moscow
127273
Russian Federation
Email: Ekaterina.Karelina@infotecs.ru