

Public-Key Cryptography Standards (PKCS) #8:
Private-Key Information Syntax Specification Version 1.2

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

IESG Note

The IESG thanks RSA Laboratories for transferring change control to the IETF. Enhancements to this specification that preserve backward compatibility are expected in an upcoming IETF standards track document.

Abstract

This document represents a republication of PKCS #8 v1.2 from RSA Laboratories' Public Key Cryptography Standard (PKCS) series. Change control is transferred to the IETF. The body of this document, except for the security considerations section, is taken directly from the PKCS #8 v1.2 specification.

This document describes a syntax for private-key information.

Table of Contents

1. Introduction	2
2. Definitions	2
3. Symbols and Abbreviations	2
4. General Overview	2
5. Private-Key Information Syntax	3
6. Encrypted Private-Key Information Syntax	4
7. Security Considerations	4
Appendix A. ASN.1 Syntax	5
Informative References	6

1. Introduction

This document describes a syntax for private-key information. Private-key information includes a private key for some public-key algorithm and a set of attributes. The document also describes a syntax for encrypted private keys. A password-based encryption algorithm (e.g., one of those described in [PKCS#5]) could be used to encrypt the private-key information.

The intention of including a set of attributes is to provide a simple way for a user to establish trust in information such as a distinguished name or a top-level certification authority's public key. While such trust could also be established with a digital signature, encryption with a secret key known only to the user is just as effective and possibly easier to implement. A non-exhaustive list of attributes is given in [PKCS#9].

2. Definitions

For the purposes of this document, the following definitions apply.

AlgorithmIdentifier: A type that identifies an algorithm (by object identifier) and any associated parameters. This type is defined in [X.509].

ASN.1: Abstract Syntax Notation One, as defined in [X.208].

Attribute: A type that contains an attribute type (specified by object identifier) and one or more attribute values. This type is defined in [X.501].

BER: Basic Encoding Rules, as defined in [X.209].

3. Symbols and Abbreviations

No symbols or abbreviations are defined in this document.

4. General Overview

The next two sections specify private-key information syntax and encrypted private-key information syntax.

This document exports two types: `PrivateKeyInfo` (Section 6) and `EncryptedPrivateKeyInfo` (Section 7).

5. Private-Key Information Syntax

This section gives the syntax for private-key information.

Private-key information shall have ASN.1 type PrivateKeyInfo:

```
PrivateKeyInfo ::= SEQUENCE {
    version                Version,
    privateKeyAlgorithm    PrivateKeyAlgorithmIdentifier,
    privateKey             PrivateKey,
    attributes              [0] IMPLICIT Attributes OPTIONAL }
```

```
Version ::= INTEGER
```

```
PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
PrivateKey ::= OCTET STRING
```

```
Attributes ::= SET OF Attribute
```

The fields of type PrivateKeyInfo have the following meanings:

version is the syntax version number, for compatibility with future revisions of this document. It shall be 0 for this version of the document.

privateKeyAlgorithm identifies the private-key algorithm. One example of a private-key algorithm is PKCS #1's rsaEncryption [PKCS#1].

privateKey is an octet string whose contents are the value of the private key. The interpretation of the contents is defined in the registration of the private-key algorithm. For an RSA private key, for example, the contents are a BER encoding of a value of type RSAPrivateKey.

attributes is a set of attributes. These are the extended information that is encrypted along with the private-key information.

6. Encrypted Private-Key Information Syntax

This section gives the syntax for encrypted private-key information.

Encrypted private-key information shall have ASN.1 type
EncryptedPrivateKeyInfo:

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

```
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
EncryptedData ::= OCTET STRING
```

The fields of type EncryptedPrivateKeyInfo have the following meanings:

encryptionAlgorithm identifies the algorithm under which the private-key information is encrypted. Two examples are PKCS #5's pbewithMD2AndDES-CBC and pbewithMD5AndDES-CBC [PKCS#5].

encryptedData is the result of encrypting the private-key information.

The encryption process involves the following two steps:

1. The private-key information is BER encoded, yielding an octet string.
2. The result of step 1 is encrypted with the secret key to give an octet string, the result of the encryption process.

7. Security Considerations

Protection of the private-key information is vital to public-key cryptography. Disclosure of the private-key material to another entity can lead to masquerades. The encryption algorithm used in the encryption process must be as 'strong' as the key it is protecting.

Appendix A. ASN.1 Syntax

```
PKCS-8 {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-8(8)
        modules(1) pkcs-8(1)}
```

```
-- $Revision: 1.5 $
```

```
-- This module has been checked for conformance with the ASN.1
-- standard by the OSS ASN.1 Tools
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
-- EXPORTS All --
-- All types and values defined in this module is exported for use in
-- other ASN.1 modules.
```

```
IMPORTS
```

```
informationFramework
    FROM UsefulDefinitions {joint-iso-itu-t(2) ds(5) module(1)
                           usefulDefinitions(0) 3}
```

```
Attribute
    FROM InformationFramework informationFramework
```

```
AlgorithmIdentifier, ALGORITHM-IDENTIFIER
    FROM PKCS-5 {iso(1) member-body(2) us(840) rsadsi(113549)
                pkcs(1) pkcs-5(5) modules(16) pkcs-5(1)};
```

```
-- Private-key information syntax
```

```
PrivateKeyInfo ::= SEQUENCE {
    version Version,
    privateKeyAlgorithm AlgorithmIdentifier {{PrivateKeyAlgorithms}},
    privateKey PrivateKey,
    attributes [0] Attributes OPTIONAL }
```

```
Version ::= INTEGER {v1(0)} (v1,...)
```

```
PrivateKey ::= OCTET STRING
```

```
Attributes ::= SET OF Attribute
```

-- Encrypted private-key information syntax

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
    encryptionAlgorithm AlgorithmIdentifier {{KeyEncryptionAlgorithms}},
    encryptedData EncryptedData
}
```

```
EncryptedData ::= OCTET STRING
```

```
PrivateKeyAlgorithms ALGORITHM-IDENTIFIER ::= {
    ... -- For local profiles
}
```

```
KeyEncryptionAlgorithms ALGORITHM-IDENTIFIER ::= {
    ... -- For local profiles
}
```

END

Informative References

- [PKCS#1] RSA Laboratories. PKCS #1: RSA Encryption Standard. Version 1.5, November 1993.
- [PKCS#5] RSA Laboratories. PKCS #5: Password-Based Encryption Standard. Version 1.5, November 1993.
- [PKCS#9] RSA Laboratories. PKCS #9: Selected Attribute Types. Version 1.1, November 1993.
- [X.208] CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.
- [X.209] CCITT. Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.
- [X.501] CCITT. Recommendation X.501: The Directory - Models. 1988.
- [X.509] CCITT. Recommendation X.509: The Directory - Authentication Framework. 1988.

Author's Addresses

Burt Kaliski
EMC Corporation
176 South Street
Hopkinton, MA 01748
USA

EMail: kaliski_burt@emc.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

