

---

# PKCS #8: Private-Key Information Syntax Standard

An RSA Laboratories Technical Note

Version 1.2

Revised November 1, 1993\*

## 1. Scope

This standard 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 standard 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. 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.

---

\*Supersedes June 3, 1991 version, which was also published as NIST/OSI Implementors' Workshop document SEC-SIG-91-23. PKCS documents are available by electronic mail to <pkcs@rsa.com>.

- 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.

### 3. Definitions

For the purposes of this standard, 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.

### 4. Symbols and abbreviations

No symbols or abbreviations are defined in this standard.

### 5. General overview

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

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

### 6. 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 standard. It shall be 0 for this version of the standard.
- ### `privateKeyAlgorithm` identifies the private-key algorithm. One example of a private-key algorithm is PKCS #1's `rsaEncryption`.
- ### `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.

## 7. 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`.

### `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.

## **Revision history**

### **Version 1.0**

Version 1.0 was distributed to participants in RSA Data Security, Inc.'s Public-Key Cryptography Standards meetings in February and March 1991.

### **Version 1.1**

Version 1.1 is part of the June 3, 1991 initial public release of PKCS. Version 1.1 was published as NIST/OSI Implementors' Workshop document SEC-SIG-91-23.

### **Version 1.2**

Version 1.2 incorporates several editorial changes, including updates to the references and the addition of a revision history.

## **Author's address**

RSA Laboratories  
100 Marine Parkway  
Redwood City, CA 94065 USA

(415) 595-7703  
(415) 595-4126 (fax)  
pkcs-editor@rsa.com