RFC 9939
PKCS #8: Private-Key Information Content Types

Abstract

This document defines PKCS #8 content types for use with PrivateKeyInfo and EncryptedPrivateKeyInfo as specified in RFC 5958.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in 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/rfc9939.

Copyright Notice

Table of Contents

1. Introduction

The syntax for private-key information was originally described in [RFC5208], and the syntax was later revised by [RFC5958] to include the AsymmetricKeyPackage content type that supports multiple PrivateKeyInfos. This document defines PKCS #8 content types for use with one PrivateKeyInfo and one EncryptedPrivateKeyInfo. These content type assignments are needed for the PrivateKeyInfo and EncryptedPrivateKeyInfo to be carried in the Cryptographic Message Syntax (CMS) [RFC5652].

Note: A very long time ago, media types for PrivateKeyInfo and EncryptedPrivateKeyInfo were assigned as "application/pkcs8" and "application/pkcs8-encrypted", respectively.

2. Private-Key Information Content Types

This section defines a content type for private-key information and encrypted private-key information.

The PrivateKeyInfo content type is identified by the following object identifier:

```
id-ct-privateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
 member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
 smime(16) ct(1) 52 }
```

The EncryptedPrivateKeyInfo content type is identified by the following object identifier:

```
id-ct-encrPrivateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
 member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
 smime(16) ct(1) 53 }
```

3. ASN.1 Module

The ASN.1 module [X680] [X690] in this section builds upon the modules in [RFC5911].

```
<CODE BEGINS>
PrivateKeyInfoContentTypes
 { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
   pkcs-9(9) smime(16) modules(0) id-mod-pkcs8ContentType(85) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL

IMPORTS

CONTENT-TYPE
 FROM CryptographicMessageSyntax-2009 -- in [RFC5911]
   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-9(9) smime(16) modules(0) id-mod-cms-2004-02(41) }

PrivateKeyInfo, EncryptedPrivateKeyInfo
 FROM AsymmetricKeyPackageModuleV1 -- in [RFC5958]
   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-9(9) smime(16) modules(0)
     id-mod-asymmetricKeyPkgV1(50) }  ;


PrivateKeyInfoContentTypes CONTENT-TYPE ::= {
 ct-privateKeyInfo | ct-encrPrivateKeyInfo,
 ... -- Expect additional content types --  }

ct-privateKeyInfo CONTENT-TYPE ::= { PrivateKeyInfo
 IDENTIFIED BY id-ct-privateKeyInfo }

id-ct-privateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
 member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
 smime(16) ct(1) 52 }

ct-encrPrivateKeyInfo CONTENT-TYPE ::= { EncryptedPrivateKeyInfo
 IDENTIFIED BY id-ct-encrPrivateKeyInfo }

id-ct-encrPrivateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
 member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
 smime(16) ct(1) 53 }

END
<CODE ENDS>
```

4. Security Considerations

The security considerations in [RFC5958] apply here.

5. IANA Considerations

For each of the private-key information content types defined in Section 2, IANA has assigned an Object Identifier (OID). The OIDs for the content types have been allocated in the "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" registry [IANA-CMS-CTS] as follows:

Decimal	Description	Reference
52	id-ct-privateKeyInfo	RFC 9939
53	id-ct-encrPrivateKeyInfo	RFC 9939

Table 1

For the ASN.1 module in Section 3, IANA has assigned an OID for the module identifier. The OID for the module has been allocated in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" registry [IANA-SMIME-MODS] as follows:

Decimal	Description	Reference
85	id-mod-pkcs8ContentType	RFC 9939

Table 2

IANA has updated the application/cms registration entry in the "Media Types" registry by adding RFC 9939 to the "Interoperability considerations" section and to the list of RFCs where Inner Content Types (ICTs) are defined (see the "Optional parameters" section) and by adding the following values to the list of ICTs:

- privateKeyInfo
- encrPrivateKeyInfo

IANA has also updated the "Security considerations" section in the application/cms entry as follows:

RFC	CMS Protecting Content Type and Algorithms
RFC 9939	privateKeyInfo and encrPrivateKeyInfo

Table 3

6. References

6.1. Normative References

[RFC5652]   Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC5911]   Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, DOI 10.17487/RFC5911, June 2010, <https://www.rfc-editor.org/info/rfc5911>.

[RFC5958]   Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <https://www.rfc-editor.org/info/rfc5958>.

[X680]   ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

[X690]   ITU-T, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.690>.

6.2. Informative References

[IANA-CMS-CTS]   IANA, "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)", <https://www.iana.org/assignments/smi-numbers>.

[IANA-SMIME-MODS]   IANA, "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)", <https://www.iana.org/assignments/smi-numbers>.

[RFC5208]   Kaliski, B., "Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2", RFC 5208, DOI 10.17487/RFC5208, May 2008, <https://www.rfc-editor.org/info/rfc5208>.

Acknowledgments

Authors' Addresses

Joe Mandel
AKAYLA, Inc.
Email: joe@akayla.com

Russ Housley
Vigil Security, LLC
Email: housley@vigilsec.com

Sean Turner
sn3rd
Email: sean@sn3rd.com