

Limited Additional Mechanisms for PKIX and SMIME
Internet-Draft
Intended status: Standards Track
Expires: 5 March 2026

J. Mandel
AKAYLA
R. Housley
Vigil Security
S. Turner
sn3rd
1 September 2025

PKCS #8 Private-Key Information Content Types
draft-ietf-lamps-pkcs8-prikeyinfo-contenttypes-01

Abstract

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

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://github.com/lamps-wg/pkcs8-PriKeyInfoCt>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-lamps-pkcs8-prikeyinfo-contenttypes/>.

Discussion of this document takes place on the Limited Additional Mechanisms for PKIX and SMIME mailing list (<mailto:spasm@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/spasm/>. Subscribe at <https://www.ietf.org/mailman/listinfo/spasm/>.

Source for this draft and an issue tracker can be found at <https://github.com/lamps-wg/pkcs8-PriKeyInfoCt>.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 March 2026.

Copyright Notice

Copyright (c) 2025 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. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Conventions and Definitions	2
3. Private-Key Information Content Types	3
4. Security Considerations	3
5. IANA Considerations	3
6. ASN.1 Module	3
7. References	4
7.1. Normative References	4
7.2. Informative References	5
Acknowledgments	5
Authors' Addresses	5

1. Introduction

The syntax for private-key information was originally described in [RFC5208] and later obsoleted by [RFC5958]. This document defines PKCS #8 content types for use with PrivateKeyInfo and EncryptedPrivateKeyInfo.

2. Conventions and Definitions

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. 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) TBD1 }
```

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) TBD2 }
```

4. Security Considerations

The security considerations in [RFC5958] apply here.

5. IANA Considerations

For the private key info content types defined in section Section 3, IANA is requested to assign an object identifier (OID) for each of the content types. The OIDs for the content types should be allocated in the "SMI Security for S/MIME CMS Content Type" registry (1.2.840.113549.1.9.16.1), and the description should be set to id-ct-privateKeyInfo (TBD1) and id-ct-encrPrivateKeyInfo (TBD2).

For the ASN.1 Module in Section 6, IANA is requested to assign an object identifier (OID) for the module identifier. The OID for the module should be allocated in the "SMI Security for S/MIME Module Identifier" registry (1.2.840.113549.1.9.16.0), and the Description for the new OID should be set to "id-mod-pkcs8ContentType".

6. ASN.1 Module

The ASN.1 module 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(TBD0) }

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) TBD1 }

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) TBD2 }

END
<CODE ENDS>
```

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/rfc/rfc2119>>.
- [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/rfc/rfc5911>>.
- [RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <<https://www.rfc-editor.org/rfc/rfc5958>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/rfc/rfc8174>>.

7.2. Informative References

- [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/rfc/rfc5208>>.

Acknowledgments

Thanks to John Gray and Deb Cooley for reviewing the document and providing comments.

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