

Internet Engineering Task Force (IETF)
Request for Comments: 5967
Updates: 2986
Category: Informational
ISSN: 2070-1721

S. Turner
IECA
August 2010

The application/pkcs10 Media Type

Abstract

This document specifies a media type used to carry PKCS #10 certification requests as defined in RFC 2986. It carries over the original specification from RFC 2311, which recently has been moved to Historic status, and properly links it to RFC 2986.

Status of This Memo

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

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc5967>.

Copyright Notice

Copyright (c) 2010 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

1. Introduction

[RFC2311] first defined the application/pkcs10 media type. When [RFC2633] was published, the application/pkcs10 section was dropped, but for some reason the text was not incorporated into the PKCS #10 document [RFC2986]. [RFC2311] was moved to Historic status by [RFC5751]. To ensure the IANA media type registration points to a non-Historic document, this document updates [RFC2986] with the definition of the application/pkcs10 media type and an IANA registration based on [RFC4288].

The text for Section 2 is adapted from Section 3.7 of [RFC2311].

1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Creating a Certification Request

A typical application that allows a user to generate cryptographic information has to submit that information to a Certification Authority (CA), who transforms it into a certificate. PKCS #10 [RFC2986] describes a syntax for certification requests.

The details of certification requests and the process of obtaining a certificate are beyond the scope of this memo. Instead, only the format of data used in application/pkcs10 is defined.

2.1. Format of the application/pkcs10 Body

PKCS #10 defines the ASN.1 type CertificationRequest for use in submitting a certification request. For transfer to a CA, this abstract syntax needs to be encoded and identified in a unique

manner. When the media type application/pkcs10 is used, the body MUST be a CertificationRequest.

A robust application SHOULD output Distinguished Encoding Rules (DER), but allow Basic Encoding Rules (BER) or DER on input.

Data produced by BER or DER is 8-bit, but some transports are limited to 7-bit data. In such cases, a suitable 7-bit transfer encoding MUST be applied; in MIME-compatible transports, the base64 encoding [RFC4648] SHOULD be used with application/pkcs10, although any 7-bit transfer encoding may work.

2.2. Sending and Receiving an application/pkcs10 Body Part

For sending a certificate-signing request, the application/pkcs10 message format MUST be used to convey a PKCS #10 certificate-signing request. Note that for sending certificates and Certificate Revocation Lists (CRLs) without any signed content, the application/pkcs7-mime message format MUST be used to convey a degenerate PKCS #7 signedData "certs-only" message [RFC5751].

To send an application/pkcs10 body, the application generates the cryptographic information for the user. The details of the cryptographic information are beyond the scope of this memo.

- Step 1. The cryptographic information is placed within a PKCS #10 CertificationRequest.
- Step 2. The CertificationRequest is encoded according to BER or DER (preferred, DER).
- Step 3. As a typical step, the encoded CertificationRequest is also base64 encoded so that it is 7-bit data suitable for transfer in ESMTP. This then becomes the body of an application/pkcs10 body part.

The result might look like this:

```
Content-Type: application/pkcs10; name=smime.p10
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p10
```

```
rfvbnj756tbBghyHhHUujhJh77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGT6rfvbnjT6jH7756tbB9H
f8HHGTrfvhJh776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V
```

A typical application only needs to send a certification request. It is a Certification Authority that has to receive and process the request. The steps for recovering the CertificationRequest from the message are straightforward but are not presented here. The procedures for processing the certification request are beyond the scope of this document.

3. IANA Considerations

IANA has updated the registration for the application/pkcs10 media subtype in the Application Media Types registry using the filled-in template from BCP 13 [RFC4288] given below.

3.1. Registration of Media Subtype application/pkcs10

The media subtype for a PKCS #10 certification request is application/pkcs10.

Type name: application

Subtype name: pkcs10

Required parameters: None

Optional parameters: None

Encoding considerations: binary; see Section 2.

Security considerations:

Clients use a certification request to request that a Certification Authority certify a public key. The certification request is digitally signed. Also, see Section 6.

Interoperability considerations: See Section 2.

Published specification: This specification.

Applications which use this media type:

Applications that support PKCS #10 certification requests [RFC2986].

Additional information:

Magic number(s): None

File extension(s): .p10

Macintosh File Type Code(s):

Person & email address to contact for further information:
Sean Turner <turners@ieca.com>

Restrictions on usage: none

Author: Sean Turner <turners@ieca.com>

Intended usage: COMMON

Change controller: The IESG

4. Security Considerations

The security considerations of [RFC2986] and [RFC5751] apply; no new security considerations are introduced by this document.

5. Acknowledgements

I wish to thank the authors of RFC 2311, Steve Dusse, Paul Hoffman, Blake Ramsdell, Laurence Lundblade, and Lisa Repka.

I would also like to thank Bjoern Hoehrmann for his review of the media subtype application.

6. References

6.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, November 2000.
- [RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", BCP 13, RFC 4288, December 2005.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

- [X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002. Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

6.2. Informative References

- [RFC2311] Dusse, S., Hoffman, P., Ramsdell, B., Lundblade, L., and L. Repka, "S/MIME Version 2 Message Specification", RFC 2311, March 1998.
- [RFC2633] Ramsdell, B., Ed., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

Author's Address

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

E-Mail: turners@ieca.com