Network Working Group
Internet-Draft
Intended Status: Informational
Expires: September 12, 2016

S. Leonard
Penango, Inc.

March 11, 2016

The PKCS #8 EncryptedPrivateKeyInfo Media Type
draft-seantek-pkcs8-encrypted-00

Abstract

This document registers the application/pkcs8-encrypted media type for use with the EncryptedPrivateKeyInfo unit of PKCS #8. This format carries an encrypted private key.

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 http://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."

1. Definitions

The key word "SHOULD" in this document is to be interpreted as described in [RFC2119].

2. Registration Application

Type name: application

Subtype name: pkcs8-encrypted

Required parameters: None.

Optional parameters:

password-mapping: When the encryption algorithm incorporates a "password" that is an octet string, a mapping between user input and the octet string is desirable. PKCS #5 [RFC2898] Section 3 recommends "that applications follow some common text encoding rules"; it then suggests, but does not recommend, ASCII and UTF-8. This parameter specifies the charset that a recipient SHOULD attempt first when mapping user input to the octet string. This parameter is not cryptographically protected, so recipients SHOULD NOT rely on it as the exclusive mapping possibility.

This parameter has similar semantics as the charset parameter from text/plain, except that it only applies to the user's input of a password. There is no default value.

The following special values are defined:

*pkcs12 = UTF-16LE with U+0000 NULL terminator (PKCS #12-style, see [RFC7292])

*precis = PRECIS password profile, i.e., OpaqueString from Section 4 of [RFC7613] (always UTF-8)

*precis-XXX = PRECIS profile as named XXX in the IANA PRECIS Profiles Registry

*hex = hexadecimal input: the input is mapped to 0-9, A-F, and then converted directly to octets. If there are an odd number of hex digits, either the final digit 0 is appended, or an error condition is raised. Compare with Annex M.4 of IEEE 802.11-2012.

dtmf = The characters "0"-"9", "A"-"D", "", and "#", which map to their corresponding ASCII codes. "A"-"D" map to the uppercase range 0x41 - 0x44. (This is to support restricted-input devices, i.e., telephones and telephone-like equipment.) User input outside of these values is either ignored, or an error condition is raised.

Otherwise, the value of this parameter is a charset, from the IANA Character Sets Registry [RFC2978].

This parameter is case-insensitive.

Encoding considerations: Binary.

Security considerations:

Carries a cryptographic private key. See Section 6 of [RFC5958].

EncryptedPrivateKeyInfo PKCS #8 data contains exactly one private key. Poor password choices, weak algorithms, or improper parameter selections (e.g., insufficient salting rounds) will make the confidential payloads much easier to compromise.

Interoperability considerations:

PKCS #8 is a widely recognized format for private key information on all modern cryptographic stacks. The encrypted variation in this registration, EncryptedPrivateKeyInfo (Section 3, Encrypted Private Key Info, of [RFC5958], and Section 6 of PKCS #8), is less widely used for exchange than PKCS #12, but it is much simpler to implement. The contents are exactly one private key (with optional attributes), so the possibility for hidden "easter eggs" in the payload such as unexpected certificates or miscellaneous secrets is drastically reduced.

Published specification:

PKCS #8 v1.2, November 1993 (republished as RFC 5208, May 2008); RFC 5958, August 2010

Applications that use this media type:

Machines, applications, browsers, Internet kiosks, and so on, that support this standard allow a user to import, export, and exercise a single private key.

Fragment identifier considerations: None.

Additional information:

Deprecated alias names for this type: N/A
Magic number(s): None.
File extension(s): .p8e
Macintosh file type code(s):
None. A uniform type identifier (UTI) of "com.rsa.pkcs-8-encrypted" is RECOMMENDED.

Object Identifiers: 1.2.840.113549.1.12.10.1.2 (when in PKCS #12)

Person & email address to contact for further information:

Sean Leonard <dev+ietf@seantek.com>

Restrictions on usage: None.

Author/Change controller: Sean Leonard <dev+ietf@seantek.com>

Intended usage: COMMON

Provisional registration? No

2. IANA Considerations

IANA is asked to register the media type application/pkcs8-encrypted in the Standards tree using the applications provided in Section 1 of this document.

3. Security Considerations

See the registration template.

4. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2898] Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0", RFC 2898, September 2000.

[RFC2978] Freed, N. and J. Postel, "IANA Charset Registration Procedures", BCP 19, RFC 2978, October 2000.

[RFC5208] Kaliski, B., "Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2", RFC 5208, May 2008.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, August 2010.

[RFC7292] Moriarty, K., Nystrom, S., Parkinson, S., Rusch, A., and M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, July 2014.

[RFC7613] Saint-Andre, P. and A. Melnikov, "Preparation, Enforcement, and Comparison of Internationalized Strings Representing Usernames and Passwords", RFC 7613, August 2015.

Author's Address

Sean Leonard
Penango, Inc.
5900 Wilshire Boulevard
21st Floor
Los Angeles, CA 90036
USA

EMail: dev+ietf@seantek.com
URI: http://www.penango.com/