Internet Engineering Task Force (IETF)
Request for Comments: 6070
Category: Informational
ISSN: 2070-1721

S. Josefsson
SJD AB

January 2011

PKCS #5: Password-Based Key Derivation Function 2 (PBKDF2) Test Vectors

Abstract

This document contains test vectors for the Public-Key Cryptography Standards (PKCS) #5 Password-Based Key Derivation Function 2 (PBKDF2) with the Hash-based Message Authentication Code (HMAC) Secure Hash Algorithm (SHA-1) pseudorandom function.

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/rfc6070.

Copyright Notice

Copyright (c) 2011 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.

Table of Contents

1. Introduction

The Public-Key Cryptography Standards (PKCS) #5 [RFC2898] Password-Based Key Derivation Function 2 (PBKDF2) is used by several protocols to derive encryption keys from a password.

For example, Salted Challenge Response Authentication Mechanism (SCRAM) [RFC5802] uses PBKDF2 with Hash-based Message Authentication Code (HMAC) [RFC2104] and Secure Hash Algorithm (SHA-1) [FIPS.180-1.1995].

Test vectors for the algorithm were not included in the original specification, but are often useful for implementers. This document addresses the shortcoming.

2. PBKDF2 HMAC-SHA1 Test Vectors

The input strings below are encoded using ASCII [ANSI.X3-4.1986]. The sequence "\0" (without quotation marks) means a literal ASCII NUL value (1 octet). "DK" refers to the Derived Key.

```
Input:
  P = "password" (8 octets)
  S = "salt" (4 octets)
  c = 1
  dkLen = 20

Output:
  DK = 0c 60 c8 0f 96 1f 0e 71
       f3 a9 b5 24 af 60 12 06
       2f e0 37 a6             (20 octets)
```

```
Input:
  P = "password" (8 octets)
  S = "salt" (4 octets)
  c = 2
  dkLen = 20

Output:
  DK = ea 6c 01 4d c7 2d 6f 8c
       cd 1e d9 2a ce 1d 41 f0
       d8 de 89 57             (20 octets)


Input:
  P = "password" (8 octets)
  S = "salt" (4 octets)
  c = 4096
  dkLen = 20

Output:
  DK = 4b 00 79 01 b7 65 48 9a
       be ad 49 d9 26 f7 21 d0
       65 a4 29 c1             (20 octets)


Input:
  P = "password" (8 octets)
  S = "salt" (4 octets)
  c = 16777216
  dkLen = 20

Output:
  DK = ee fe 3d 61 cd 4d a4 e4
       e9 94 5b 3d 6b a2 15 8c
       26 34 e9 84             (20 octets)


Input:
  P = "passwordPASSWORDpassword" (24 octets)
  S = "saltSALTsaltSALTsaltSALTsaltSALTsalt" (36 octets)
  c = 4096
  dkLen = 25

Output:
  DK = 3d 2e ec 4f e4 1c 84 9b
       80 c8 d8 36 62 c0 e4 4a
       8b 29 1a 96 4c f2 f0 70
       38                      (25 octets)
```

```
   Input:
     P = "pass\0word" (9 octets)
     S = "sa\0lt" (5 octets)
     c = 4096
     dkLen = 16

   Output:
     DK = 56 fa 6a a7 55 48 09 9d
          cc 37 d7 f0 34 25 e0 c3 (16 octets)
```

3. Acknowledgements

Barry Brachman and Love Hornquist Astrand confirmed the test vectors (using independent implementations) and pointed out a mistake in the salt octet length count.

4. Copying Conditions

This document should be considered a Code Component and is thus available under the BSD license.

5. Security Considerations

The security considerations in [RFC2898] apply. This document does not introduce any new security considerations.

6. References

6.1. Normative References

[ANSI.X3-4.1986]
American National Standards Institute, "Coded Character Set - 7-bit American Standard Code for Information Interchange", ANSI X3.4, 1986.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

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

[FIPS.180-1.1995]
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

6.2. Informative References

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, July 2010.

Author's Address

Simon Josefsson
SJD AB
Hagagatan 24
Stockholm 113 47
SE

EMail: simon@josefsson.org
URI: http://josefsson.org/