

---

Stream: Internet Engineering Task Force (IETF)  
RFC: [9879](#)  
Obsoletes: [9579](#)  
Updates: [7292](#), [8018](#)  
Category: Informational  
Published: September 2025  
ISSN: 2070-1721  
Author: A. Kario  
*Red Hat, Inc.*

# RFC 9879

## Use of Password-Based Message Authentication Code 1 (PBMAC1) in PKCS #12 Syntax

---

### Abstract

This document specifies additions and amendments to RFCs 7292 and 8018. It also obsoletes the RFC 9579. It defines a way to use the Password-Based Message Authentication Code 1 (PBMAC1), defined in RFC 8018, inside the PKCS #12 syntax. The purpose of this specification is to permit the use of more modern Password-Based Key Derivation Functions (PBKDFs) and allow for regulatory compliance.

### 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 candidates for any level of Internet Standard; see 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/rfc9879>.

### 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	3
1.1. Changes since RFC 9579	3
2. Rationale	3
3. Requirements Language	3
4. Embedding PBMAC1 in PKCS #12	4
5. Recommended Parameters	4
6. Password Encoding	4
7. Deprecated Algorithms	5
8. IANA Considerations	5
9. Security Considerations	5
10. References	5
10.1. Normative References	5
10.2. Informative References	6
Appendix A. Test Vectors	7
A.1. Valid PKCS #12 File with SHA-256 HMAC and PRF	7
A.2. Valid PKCS #12 File with SHA-256 HMAC and SHA-512 PRF	8
A.3. Valid PKCS #12 File with SHA-512 HMAC and PRF	9
A.4. Invalid PKCS #12 File with Incorrect Iteration Count	10
A.5. Invalid PKCS #12 File with Incorrect Salt	12
A.6. Invalid PKCS #12 File with Missing Key Length	13
Appendix B. ASN.1 Module	14
Author's Address	16

## 1. Introduction

The PKCS #12 format [RFC7292] is widely used for the interoperable transfer of certificate, key, and other miscellaneous secrets between machines, applications, browsers, etc. Unfortunately, [RFC7292] mandates the use of a PKCS #12 specific password-based key derivation function that only allows for change of the underlying message digest function.

### 1.1. Changes since RFC 9579

This document changes the specified format of the password passed to the key derivation function. Previously, it was a BMPString, but now it's declared as a UTF8String. It should be noted that the test vectors attached to [RFC9579] use UTF8String encoding. This resolves [Err7974].

## 2. Rationale

Due to security concerns with the key derivation function from [RFC7292] and the much higher extensibility of PBMAC1 [RFC8018], we propose the use of PBMAC1 for integrity protection of PKCS #12 structures. The new syntax is designed to allow legacy applications to still be able to decrypt the key material, even if they are unable to interpret the new integrity protection, provided that they can ignore failures in Message Authentication Code (MAC) verification. This change allows for the use of PBKDF2 [RFC8018] or scrypt PBKDFs [RFC7914] for derivation of MAC keys and future extensibility. Use of the extensible PBMAC1 mechanism also allows for greater flexibility and alignment with different government regulations, for example, in environments where PBKDF2 is the only allowed password-based key derivation function.

As the recommended methods for key protection require both encryption and integrity protection, we decided to amend the PKCS #12 format to support different key derivation functions rather than extending the PKCS #5 format by a new field that allows integrity protection.

We included an ASN.1 module [x680] [x681] [x682] [x683] [x690] that can be combined with the ASN.1 modules in [RFC7292] and [RFC8018] to incorporate additional MAC algorithms.

## 3. Requirements Language

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.

## 4. Embedding PBMAC1 in PKCS #12

The MacData structure in the PFX object, as described in item #3 in [Section 4](#) of [\[RFC7292\]](#), is updated to include the following PBMAC1-specific guidance:

- a. The id-PBMAC1 object identifier is permitted as a valid type for the DigestAlgorithmIdentifier inside the DigestInfo object. If the algorithm field of the DigestAlgorithmIdentifier is id-PBMAC1, then the parameters field **MUST** be present and have a value consistent with PBMAC1-params parameters.
- b. If the PBMAC1 algorithm is used, the digest value of the DigestInfo object **MUST** be the result of the PBMAC1 calculation over the authSafe field using the PBMAC1-params parameters.
- c. If the PBMAC1 algorithm is used, the macSalt value **MUST** be ignored. For backwards compatibility, it **SHOULD NOT** be empty.
- d. If the PBMAC1 algorithm is used, the iterations value **MUST** be ignored. For backwards compatibility, it **SHOULD** have a non-zero positive value.

## 5. Recommended Parameters

To provide interoperability between different implementations, all implementations of this specification **MUST** support the PBKDF2 key derivation function paired with SHA-256 HMAC [\[SHA2\]](#) [\[RFC2104\]](#) for both integrity check and the PBKDF2 pseudorandom function (PRF). It's **RECOMMENDED** for implementations to support other SHA-2-based HMACs. Implementations **MAY** use other hash functions, like the SHA-3 family of hash functions [\[SHA3\]](#). Implementations **MAY** use other KDF methods, like the script PBKDF [\[RFC7914\]](#).

The length of the key generated by the used KDF **MUST** be encoded explicitly in the parameters field and **SHOULD** be the same size as the HMAC function output size. This means that PBMAC1-params specifying SHA-256 HMAC should also include KDF parameters that generate a 32-octet key. In particular, when using the PBKDF2, implementations **MUST** include the keyLength field in the encoded PBKDF2-params. Implementations **MUST NOT** accept PBKDF2 KDF with PBKDF2-params that omit the keyLength field.

## 6. Password Encoding

As documented in [Appendix B.1](#) of [\[RFC7292\]](#), the handling of password encoding in the underlying standards is underspecified. However, unlike with Password-Based Encryption Scheme 1 (PBES1) [\[RFC8018\]](#) when used in the context of PKCS #12 or the MAC algorithm described in [\[RFC7292\]](#) (which use BMPString with NULL termination), all passwords used with PBMAC1 **MUST** be created from UTF-8 encoding [\[RFC3629\]](#) without a NULL terminator or Byte Order Mark (BOM).

## 7. Deprecated Algorithms

While attacks against SHA-1 HMACs are not considered practical [RFC6194] to limit the number of algorithms needed for interoperability, implementations of this specification **SHOULD NOT** use PBKDF2 with the SHA-1 HMAC. In addition, implementations **MUST NOT** use any other message digest functions with an output of 160 bits or less.

## 8. IANA Considerations

IANA has registered the following object identifier in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" registry. See [Appendix B](#) for the ASN.1 module.

IANA has updated the reference to point to this document.

Decimal	Description	Reference
76	id-pkcs12-pbmac1-2023	RFC 9879

Table 1

## 9. Security Considerations

Except for the use of different key derivation functions, this document doesn't change how the integrity protection on PKCS #12 objects is computed; therefore, all the security considerations from [RFC7292] apply.

Use of PBMAC1 and PBKDF2 is unchanged from [RFC8018]; therefore, all the security considerations from [RFC8018] apply.

The KDFs generally don't have a lower limit for the generated key size, allowing the specification of very small key sizes (of 1 octet), which can facilitate brute-force attacks on the HMAC. Since the KDF parameters are not cryptographically protected and HMACs accept arbitrary key sizes, implementations **MAY** refuse to process KDF parameters that specify small key output sizes or weak parameters. It's **RECOMMENDED** to reject any KDF parameters that specify key lengths less than 20 octets.

## 10. References

### 10.1. Normative References

- [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <<https://www.rfc-editor.org/info/rfc2104>>.

- [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/info/rfc2119>>.
- [RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <<https://www.rfc-editor.org/info/rfc3629>>.
- [RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <<https://www.rfc-editor.org/info/rfc6194>>.
- [RFC7292] Moriarty, K., Ed., Nystrom, M., Parkinson, S., Rusch, A., and M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, DOI 10.17487/RFC7292, July 2014, <<https://www.rfc-editor.org/info/rfc7292>>.
- [RFC8018] Moriarty, K., Ed., Kaliski, B., and A. Rusch, "PKCS #5: Password-Based Cryptography Specification Version 2.1", RFC 8018, DOI 10.17487/RFC8018, January 2017, <<https://www.rfc-editor.org/info/rfc8018>>.
- [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/info/rfc8174>>.
- [SHA2] NIST, "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015, <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>>.
- [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>>.
- [x681] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Information object specification", ITU-T Recommendation X.681, ISO/IEC 8824-2:2021, February 2021, <<https://www.itu.int/rec/T-REC-X.681>>.
- [x682] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification", ITU-T Recommendation X.682, ISO/IEC 8824-3:2021, February 2021, <<https://www.itu.int/rec/T-REC-X.682>>.
- [x683] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications", ITU-T Recommendation X.683, ISO/IEC 8824-4:2021, February 2021, <<https://www.itu.int/rec/T-REC-X.683>>.
- [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>>.

## 10.2. Informative References

- [Err7974]** RFC Errata, Erratum ID 7974, RFC 9579, <<https://www.rfc-editor.org/errata/eid7974>>.
- [RFC7914]** Percival, C. and S. Josefsson, "The scrypt Password-Based Key Derivation Function", RFC 7914, DOI 10.17487/RFC7914, August 2016, <<https://www.rfc-editor.org/info/rfc7914>>.
- [RFC9579]** Kario, H., "Use of Password-Based Message Authentication Code 1 (PBMAC1) in PKCS #12 Syntax", RFC 9579, DOI 10.17487/RFC9579, May 2024, <<https://www.rfc-editor.org/info/rfc9579>>.
- [SHA3]** NIST, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", FIPS PUB 202, DOI 10.6028/NIST.FIPS.202, August 2015, <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>>.

## Appendix A. Test Vectors

All test vectors use "1234" as the password for both encryption and integrity protection.

### A.1. Valid PKCS #12 File with SHA-256 HMAC and PRF

The following base64-encoded PKCS #12 file **MUST** be readable by implementations following this RFC.

```
MIIKigIBAzCCCgUGCSqGSIB3DQEHAaCCCFYEggnymIIJ7jCCBGIGCSqGSIB3DQEH
BqCCBFMwggRPAgEAMIIIESAYJKoZIhvcNAQcBMFcgGSqGSIB3DQEFDTBKMCKGCSqG
SIb3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBg1ghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPHVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWMxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8g0zBMFf6BpXf/3xWAJtxyic+tSNETF0Ja8zTZb0+1V0w9
5eUmDrPUpxEVbb0KJtIc63gRkcfRptDd6Ii4Zzbzj2Evr4/S4hnrQBsiyVzJWY
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDC0yOZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLkmZoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQ1hJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46h0f4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0Qc0i29/M9WwFlo4urePyI8PK2qtVampD3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQq0jsQCxVz9i9K8NDeD
aaU98VA10To2sk3/VR/QUq0PRwU1jPN5BzUevhE7S0y/ImuJKwpGqqF1jYdrQmj5
jDe+LmYH9QGVRlfn8zuU+48FY8CAoeBeHn5AAPm10PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwk+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWeKj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
lDoXvvS3NqsnTXHcn3T9tkPROee6L7Dh3x40d961cRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF
c7hLNquuaF4qoDaVwYXHH3iuX6YlJ/3siTKbYCVXPEZ0AMP91F/OU76UMJBQNFU
0xjDx+3AhUVgnGuCsmYlK6ETDp8q0ZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkcZHi4C2fXnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXdtwqEuvzGHLVFsCuAde40ZFBmtBrf70wG7Zk08SUZ8Zz1IX3+S024g7yJ
QRev/6x6TtkwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFCGCSqGSIB3DQEFDTBKMCKGCSqGSIB3DQEFDDAcBAHtxzw+
VptrYAIICCAAwDAYIKoZIhvcNAgkFADAdBg1ghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdtQEggTQzCwI7j34gCTvfj6nuOSndAjShGv7mN2j7WMV0ps1Tpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pd0cfCnEpMFccNv2sQrLp1m0CKXu80jSqHZLoKVL0R0VsZ
```

```

8dMECLLigDlPKRiSyLEr114tErX4/zbkUaWMR0028kFbTbubQ8YoHlRUwsKW1xLg
vfi0gRkG/zHXRFQHjX/8NStv7hX1ehn7/Gy2EKPsRFhadm/iUHAfmCMkMgHTU248
JER9+nsX1td59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGHMBPVwbVUD
A40CiQBVdCoGtPjya1L28xoS3H0ILFCnwQ0r6u0HwleNJPgHq78HUyH6Hwxnh0b0
5o163r6wTFZn5cM0xpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
T4JhZ0h/CfcV2WWvhpQugkY0pWrZ+EMneB1dZB96mJVLx0i1480eSgi0PsxZMni
YM33rTpwQT5Wq0sEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1Lcq0dr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HDlFBw2Yzp9iadv4Kmb2MzhStLUoi2MSjvnnkKd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKkEVF9JBtxCR4JEn6C98Lpg+Lk+rFY7gH0f
ZxtgGURwgXRY3aLURdT55ZKkg3ExVKPzi5EhdpAau7JKhp0wyKozAp/OKWMNRz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgVvaA8pZCYqxxjpLjSJR8B
Bu9H9xkTh7K1hxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF
W6PJbucP0YPp00VtWtQdZZ3df1P0hZ7qvKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
wjNzoDM2QT+UUKJiGYXJUE009hXzFHlGj759DcNRhpgl5AgR57ofISD9yBuCAJY
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaL0XfzyfyaSmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82
HhggcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYPJdyoaX7tDmVc1Lhw19ps/
0841pIsNLJWXwvxG6B+3LN/kw4QjwN194Popi0D7+oDm5mhtT078CrBrRxHMD/0Q
qniZjKzSzEpxLzq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/BlnxN9eKbdT0i2wIi64h2QG8n0k66wQ/PSIJYwZl6eDNEQsZH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqVvPGXZD0
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiig3guhdeyRVf100x369kKwCg75q77hxE
IzSzDyUlBNbnom9SIjUt3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsY0kdZ4PYa9XPUZxXFagZsoS3F1sU799+IJVU0tC0MEXJTAjBgkq
hkiG9w0BCRUxFgQUwW05DorvVWYF3BWUmAw0rUEajScwFDBtMEkGCSqGSiB3DQEF
DjA8MCwGCSqGSiB3DQEFDDAfBAhvRzw4sC4xcwICCAACASAwDAYIKoZIHvcNAgkF
ADAMBggqhkiG9w0CCQUABCb6PW2F0dcCNj87zS64NUXG36K5aXDNFhctIk5Bf4kG
3QQITk9UIFVTRUQCAQE=

```

## A.2. Valid PKCS #12 File with SHA-256 HMAC and SHA-512 PRF

The following base64-encoded PKCS #12 file **SHOULD** be readable by implementations following this RFC.

```

MIIKigIBAZCCCgUGCSqGSiB3DQEHAaCCCFYEggnymIIJ7jCCBGIGCSqGSiB3DQEH
BqCCBFMwggRPAgEAMIIIESAYJKoZIhvcNAQcBMFfcGCSqGSiB3DQEFDTBKMCKGCSqG
SiB3DQEFDDAcBAi4j6UBBY2i0gICCAAwDAYIKoZIHvcNAgkFADAdBg1ghkgBZQME
ASoEEFpHSS5zrk/9pkDo1JRbtE6AggPgtbMLGoF5KLpVXMdcxLrT129L7/vCr0B
0I2tnhPPA7aFtRjjuGbwooCMQwxw9qzuCX1eH4xK2LUw6Gbd2H47WimSOWJMaiUb
wy4a1IWELyufe74kXPmKPCyH92lN1hqu8s0EGhI17nBhWbFzow1+qpIc9/lpujJo
wodSY+pNBD8oBeoU1m6Dg0jgc62apL7m0nwavDUQet7HAqtTBxKxu/3lpb1q8nb1
XLtQR0ax5feXerf+GQAqs24hUJIPg301eCMDVzH0h5pgZyRN9ZSIP0HC1i+d1lnb
JwHyrAhZv8GMdAVkAXHETbq8zTpxT3UE/LmH1gyZG0G2B21D2dvNDKa712sHOS/t
3XkFngHDLx+a9pVftt6p7Nh6jqI581tb7fyc7HBV9VUc/+xGgPghZouaZw+I3PUz
fjHboyLQer22ndBz+11/S2GhhZ4xLXg4l0ozkgn7DX92S/UlbmcZam1apjGwkGY/
7ktA8BarNW211mJF+Z+hci+BeDiM7eyEguLCYRdH+/UBiUuYjG1hi5Ki3+42pRZD
FZkTHG0rcG6qE2KJDsENj+RkGiylG98v7f1m4iWfVAB78A1AogT38Bod40evR70k
c48s0IW05eCH/GLS00MHKcttYUQNMqIdiG1TLzP1czFghhG97AxITzYkKLx2cYfs
pgg5PE9drq1fNzBZMUmC2bSwRhGRb5PDU6meD8uqvjxoIIZQAEV53xmD63umLUH1
jhVXfcWSmhU/+vV/IWStZgQbwhF7DmH2q6S8itCkz7J7Byp5xcDiU0Z5Gpf9Rjnk
DTZo0YM5iA8kte6KCwA+jmCgstI5EbRbnsNcJnVat3q/X776VdmnehW0VeL+6k4
z+GvQkr+D2sxPldIb5hrb+1rcp9nOQgtpBnbXaT16Lc1HdTNe5kx4ScujX0Wwfd
Iy6bR6H0QFq2SLKAAC0qw4E8h1j3WPx119e0FXNtoRKdsRuX3jzyqDBrQ6oGskL
wnyMtVjSX+3c9xbFc4vyJPFMPwb3Ng3syjUDrOpU5RxaMEAWt4josadWKEeyIC2F
wrS1dzFn/5wv1g7E7xWq+nLq4zdppsyY01jzNubh0EtJ2lhme3NJ45fxnxXmrPku

```



```

gBda1lLf29inVuzuTjwLjQwGk+usHJm9R/K0hTaSNRgepXnjY0cIgS+0gEY1/BW
k3+Y4GE2JXds2cQToe5rCSYH3QG0QTYUAGvWx6hAlhrRRgUG3vxtYSixQ3UUwzs
eQW2SUFLL1611lJ7cQwFSPyr0sL0p81vdxWiigwjkfPtgljZ2QpmzR5rX2xiqItH
Dy4E+iVigIYwggWEBGkqhkiG9w0BBWGGggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAQCCBTEwggUtMFCGCSqGSIB3DQEFDTBKMCKGCSqGSIB3DQEFDDAcBAHdiwsh
4wt3aAICCAAwDAYIKoZIhvcNAgkFADAdBglgghkgBZQMEASoEELNFnEpJT65wsXwd
fZ1g56cEggTQRo04bP/fWfPPZrTEczq1q01HHV86j76Sgxau2WQ90QAG998HFtNq
Nx08R66en6QFhqpWCI73tSJD+oA29q0sT+Xt2bR2z5+K7D4QoiXuLa3gXv62VkjB
0DLCHAS7Mu+hkp50KCpXCS7fo00nAiQjM4EluAsiwwLrHu7z1E16UwpmLgKQnaC1
S44fV9znS9TxfRTnuCq1lupdn2qQjSyd0U6inQeKLBf1KRiLrJHOobaFmjWwp1U
OQAMuZrAlhHyIb0FXMPYk3mmU/1UPuRGcbcV5v2Ut2UME+WYExXSCOYR3/R4UfVk
IfEzeRPfs2s1JMIDS2fmMyFkEEE1BckhK09IzhQV3koeKUBdM066ufyax/uIyXPm
MiB9fAqbQQ4jkQTt80bKkBAp1Bvyg2L8BssstR5iCoZgWnfA9Uz4RI5GbRqbCz7H
iSkU0IowEq0ox3IwBxty5VdWBXNjZBhpbE0CyMLSH/4QdGvW8R0DiCAC0mmaMaZq
32yrBR32E472N+2KaicvX31MwB/LkZN46c34TGanL5LJZx0DR6ITjdNgP8T1SSrp
7y2mqi7VbKp/C/28Cj5r+m++Gk6EOUpLHsZ2d2hthrr7xqoPzUAEkkyYWedHJaoQ
TkoIisZb0MGLXb9thjQ8Ee429ekfjv7CQfSDS6KTE/+mhuJ33mPz1ZcIacHjdHhE
6rbrKhjSrLbgmrGa8i7ezd89T4EONu0wkG9KW0wM2cn5Gb12PF6rxjTfzypG7a50
yc1IJ2Wrm0B7gGuYpVoCeIohr7I1xPYdeQGR0/SlzTd0xYaJVm9FzJaMNK0ZqnZo
QMEPaeq8PC3kMjpa8eAiHXk9K3DWD0WYviGVCPVYIZK6Cpwe+EwfXs+2hZgZ1Yzc
vpUWg60md1PD4UusyLQagaj37ubR6K4C4mzlhF5xNovV/C/KD+LgekMbjCtweQeWy
agev219KUEz73/BT4TgQFM5K2qZpVamwms0mldPpekGPiUCu5YxYg/y4jUKvAqj1
S9t4wUAScCJx80vXUfGpmS2+mhFPBiFps0M403nWG91Q6mKMqbNHPUCFDn9P7cUh
s1xu3NRLyJ+QIfVfba3YBTv8A6WBYEmL9lxf1uL1WS2Bx6+Crh0keyNUPo9cRjpx
1oj/xkInoc2HQ0DEkvuK9DD7VrLr7sDhfmJvr1mUfJMq5/THk7Z+E+NAuMdmTKM2
yKXxghZAbBrQkU3mIW150i7PsjlUw0o0/LJvQwJIsh6yeJDHY8mby9mIdeP3LQAF
c1YKzNwmgwbdtmVAXmQxLuhmEpXfstIzkBrNjZchzb2onNSfa+r5L6XEHNH17wCw
TuuV/JWldNuYXLfvfuv3msfSjSWkv6aRtRWIvm0v0Qba2o05L1wFmd1PzKM5uN4D
DYtsS9A6yQOXEsvUkWcLOJnCs8SkJRdXhJTxmzmeBqM1JttKwLbgGMbpjbxlg3ns
N+Z+sEFox+2ZW0glgnBHj0mCZOiAC8wqUu+sxsLT4WndaPWKVqoRQChvDaZaNoaN
qHciF9HPUCfZow+fH8TnSHneiQcDe6XcMhSaQ2MtpY8/jrgNKguZt22yH9gw/VpT
3/QOB7FBgKfIEbvUaf3nVjF1lryIheg+LeiBd2isoMNNXaBwgc2YXukxJTAjBgkq
hkiG9w0BCRUxFgQUwW05DorvVWYF3BWUmAw0rUEajScwFDBtMEkGCSqGSIB3DQEF
DjA8MCwGCSqGSIB3DQEFDDAfBAgUr2yP+/DBrgICCAACASAwDAYIKoZIhvcNAgsF
ADAMBggqhkiG9w0CCQUABCA5zFL93jw8ItG1cbHKhqkNwbgpp6layuOuxSju4/Vd
6QqITk9UIFVTRUQAQE=

```

### A.3. Valid PKCS #12 File with SHA-512 HMAC and PRF

The following base64-encoded PKCS #12 file **SHOULD** be readable by implementations following this RFC.

```

MIIKrAIBAZCCCgUGCSqGSIB3DQEHAaCCCFYEggnymIIJ7jCCBGIGCSqGSIB3DQEH
BqCCBFMwggRPAgEAMIIIESAYJKoZIhvcNAQcBMFCGCSqGSIB3DQEFDTBKMCKGCSqG
SIB3DQEFDDAcBAisrql8obSBAQICCAAwDAYIKoZIhvcNAgkFADAdBglgghkgBZQME
ASoEECjXYYca0pwsn1Imb9WqFGAggPgT7RcF5YzEJANZU9G3tSdpCHnyWatTlhm
iCEcBGgwI5gz0+GoX+JCojgYY4g+KxeqznyCu+6GeD00T4Em7SWme9nzAfBFzng0
3lYCSnahSEKfgHerbzAtq9kgXkc1PVk0Liy92/buf0Mqotjjs/5o78AqP86Pwbj8
xYNUXOU1iv00JiW2c2HefKYvUvMY10h99LCoZPLHPkaaZ4scAwDjFeTICU8oowVk
LKvs1rg1pHbfxHMFJ4yqub37hRtj2CoJNy4+UA2hBYlBi9WnuAJIsjv0qS3kpLe
4+J2DGe31NG8pD01XD016901a1k1ykh4ap2u0KeD2z357+trCFbpWMMXQcSUC0
OcVjYqgv/11++9hu0HoPSt224x4wZfJ7c02zbAAx/K2CPhdvi4CBaDHADsRq/c8
SAi+LX5SCocGT51zL5KQD6pnr2ExaVum+U8aMPPMv9R2MfFUKsYNGgFvS+lcZf
R3qk/G9iXtSgray0mwRA8pWzoX143vc9HJuuCU+ry0c/h36NChhQ91tivUNaiUc2
b9AAQsrZD8Z7KtxjBH3noS+gJdtimDB0Uh199zaCwQ95y463zdYsNCESm10T979o

```

```

Y+81BWFMM/Hog5s7Ynhoi2E9+ZlyLK2UeKwvWjGzvcdPvxHR+5l/h6PyWR0lpaZ
znmZBm+NKmbXtMD2AEa5+Q32ZqJQhijXZYIji3NS65y81j/a1ZrvU0lOVKA+MSPN
KU27/eKZuF1LEL6qaazTUmpznLLdaVQy5aZ1qz5dyCziKcuHIc1hh+RCb1HU6XdE
6pUTZSRQqiGUiKPUTnU9SF1Zc7VwvxgeynLyXPCsZ0KNWYGajy1LxDvv28uhMgNd
WF51bNk11QYl0fNunG07Yft4wk+g7CQ/Yu2w4P7S3ZLMw0g4eYclcvyIMt4vxXfp
VTKIPyzMqLr+0dp1eCPm8fIdaBZUhmUC/OVqLwgnPNY9cXCrn2R1cGKo5LtvjtjbH
2skz/D5DI0ErFzSBJ8LE3De4j8MAj0eC8ia8LaM4PNfW/noQP1LBSztTDTqEy01N
Z5uliIocYqzlyWChErJv/Wxh+zBpbk1iXc20wmh2GKjx0VSe7XbiqdoKkONUNUIE
siseASiU/oXdJYUnBYVEUDJ1HPz7qnKiFhSgxNJZnoPfzbbx1hEzV+wxQqNnWIqQ
U0s7Jt22wDBzPBHGao2tnGRLuBZWVePJGbsxThGKwrf3vYsNJTxme5KJiaxcPMwE
r+l2n2AqV0zzXHXgIxv/dvK0Qa7pH3AvGzcfjQChTRippqiRrLor0//8580h+Ly2l
IFo7bCuztmcwggWEBgkqhkiG9w0BBWgGggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTewggUtMfcGCSqGSIB3DQEFDTBKMCKGCSqGSIB3DQEFDDAcBAI1c7S5
IEG77wICCAAwDAYIKoZIhvcNAgkFADAdBg1ghkgBZQMEASoEEN6rzRtIdYxqOnY+
aDS3AFYEggTQNdUoZDXCry0FBUI/z71vfoYAxlnwJLRHNXQU1I7w0KkH22aNNsm
xiaXHoCP1HgcmsYORS7p/ITi/9atCHqnGR4zHmePNhoMpnHfEhdj1UuWgt004vUJ
5ZwTdXwem+K4We6CfWA/tyvsyGNAsuune1+8243Zsv0mGLKpjA+ZyALt51s0knmX
OD2DW49FckImUVnNC5LmvEIAMVC/ZNycryZQI+2EBkJKe+BC3834GexJnSwtUBg3
Xg33ZV7X66kw8tK1Ws5zND5GQAjyIu47mnjZkIWQBY+XbWowrBZ8uXIQuXmZC0p8
u62oIAtZaVQoVTR1LyR/7PISFW6ApwtbTn6uQxsb16qF81EM0S1+x0AfJY6Zm11t
yCqbb2tYZF+X34MoUkR/IYC/KCq/KJdpnd8Yqgfrwjg8dR2WGIxpb2GBHq6BK/DI
eh0LMcLcsOuP0DEXppfcelMOGNI+s4h4KsjWiHVDMPsqLdozBdm6FLGcno31Y5F0
+avVr1E1A0B+9evgaBbD21SrEMOjAOD090tgXXwYBEnWnIpdK+56cf5IpshrLBA
/+H13LBLEs+X1o5dd0Mu+3abp5RtAv7zLPRRtXkDYJPzgNcTvJ2Wxw2C+zrAcLzZ
7IRdcLESUa4CsN01aEvQg0tkCNVjSctkJGP0FstsWM4hP7lfsB7P2tDL+ugy6GvB
X1sz9fMC7QMAFL98nDm/yqcnejG1BcQXZho8n0svSfbcVByG1PZGMuI9t25+0B2M
TAX0f6zoD8+fFmhcVgS6MQPybGKFawckYl0zulsePqs+G4voIW17owGksRiv06Jm
ZSwD3KoGmjM49ADzuG9yrQ5PSa0nhVk1tybNape4HNYHrAmmN0IL1N+E0Bs/Edz4
ntYZuoc/Z35tCgm79dV4/Vl6HUZ1JrLsLrEWCBYvtwVFyf3/MwTWdf+Ac+XzBuC
yEMqP1vnPWswdnaid35pxios79fP11Hr0/Q6+DoA5GyYq8SFdP7EYLrGMGa5GJ+x
5nS7z6U4UmZ2sXuKYHnuhB0zi6Y04a+fhT71x02eTeC7aPlEB319UqysujJVJnso
bkcwOu/Jj0Is9YeFd693dB44xeZuYyv1woD19lqcm0Tsa2Tw7D1W/yu47dKrVP2
VKxRqomuAQ0poZiuSfq1/7ysrV8U4hI1IU2vnrSVJ8EtPQKsoBW5170dQGwXyxBk
BUTHqfJ4LG/kPGRM0tUzggFw2DjJtbym1q1MZgp2ycMon4vp7DeQLGs2XfEANB+Y
nRwtjpevqAnIuK6K3Y02LY4FXTNQpC37Xb04bmdIQAcE0MaoP4/hY87aS82PQ68g
3bI79uKo4we2g+WaEJlEzQ7147ZzV2wbDq89W69x1MWTfaDw1Etd4UaacYchAv7B
TVaaVFIRAUyWwAhGePpZG2WV1feH/zd+temxWR9qMfGbzYsg1jipBPVciw10Lq1W
s/raIBYmLmAmmGm3759UkNVznDoFhrY4z2EADxp0RHHVzJS1x+yYvp/9I+AcW55
oN0UP/3uQ6eyz/ix22sovQwhMJ8rmgR6CfyRPKmXu1RPK3puNv7mbFTfTXpYN2vX
vhEZReXy8hJF/9o4G3UrJ1F0MgUHMCG86cw1z0bhPSaXVoufOnx/fRoxJTAjBqkq
hkiG9w0BCRUxFgQUwW05DorvVWYF3BwUmAw0rUEajScwgZ0wgY0wSQYJKoZIhvcN
AQUOMDwwLAYJKoZIhvcNAQUUMMB8ECFdaXOUa0cUPAgIIAAIBQDAMBggqhkiG9w0C
CwUAMAwGCCqGSIB3DQILBQAEQHIAM8C9OAsHUCj9Cm0Jioqf7YwD40/b3UiZ3Wqo
F60mQIRdc68SdKzJ602414nW1nhTE7a41b2Tru4k3N0Ta1oECE5PVCBVU0VEAgEB

```

### A.4. Invalid PKCS #12 File with Incorrect Iteration Count

The following base64-encoded PKCS #12 file **MUST NOT** be readable by an implementation following this RFC when it is verifying integrity protection.

```

MIIKiwIBAzCCCgUGCSqGSIB3DQEHAaCCCfYEggnymIIJ7jCCBGIGCSqGSIB3DQEH
BqCCBFMwggRPAgEAMIIIESAYJKoZIhvcNAQcBMFcgCSqGSIB3DQEFDTBKMCKGCSqG
SIB3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBg1ghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPhVTWVHD+kIss+jssj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb

```

+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF  
Fj75NrIbmNiDMCb71Q8gOzBMFf6BpXf/3xWAJtxyic+tSNETF0Ja8zTZb0+lv0w9  
5eUmDrPUpxEVbb0KJtIc63gRkcfRptDd6Ii4Zzbzj2Evr4/S4hnrQBsirVzJWY  
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDC0yOZWC4n5wHLtYyhR6JaElxbrhxP  
H46z2USLkmZoF+YgEqGycSBXMgP0t36+XqocFWYi2N5niy02TnctwF430FYsQlhJ  
Suma4I33E808dJuMv8T/soF66HsD4Zj46h0f4nWmas7IaoSAbGKXgIa7KhGRJvij  
xM3W0X0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh  
nbGjGiUk4h0Qc0i29/M9WwFlo4urePyI8PK2qtVAmpD3rTLlsmgzguZ69L0Q/CFU  
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQq0jsQCxVz9i9K8NDeD  
aau98VA10To2sk3/VR/QUq0PRwU1jPN5BzUevhE7S0y/ImuJKwpGqqFljYdrQmj5  
jDe+LmYH9QGVRlfn8zuU+48FY8CAoeBeHn5AAPm10PYPVUnt3/jQN1+v+CahNVI+  
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPwmn3w75ZIA  
MJrXWekj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r  
lDoXvvS3NqsnTXHcn3T9tkPROee6L7Dh3x40d96lcRwgdYT5BwyH7e341d4VTUmJ  
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF  
c7hLNquuaF4qoDaVwYXHH3iuX6YlJ/3siTKbYCVXPEZOAMBP91F/OU76UMJBQNFU  
0xjDx+3AhUVgnGuCsmYlK6ETDp8q0ZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0  
X9fMkcZHi4C2fxnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4  
wP/VqXdqTqwEuvzGHLVfScuAde40ZFBmtBrf70wG7Zk08SUZ8Zz1IX3+S024g7yJ  
QRev/6x6TtkwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBw0wggVpBgsqhkiG9w0B  
DAoBAqCCBTewggUtMfcGCSqGSIB3DQEFDTBKMCKGCSqGSIB3DQEFDDAcBAHtxzw+  
VptrYAIcCAAwDAYIKoZIhvcNAgkFADAdBg1ghkgBZQMEASoEEK9nSqc1I2t4tMVG  
bWHpdTQEGgTQzCwI7j34gCtvfj6nuOSndAjShGv7mN2j7WMV0ps1Tpq2b9Bn3vn1  
Y0JMvL4E7sLrUzNU02pd0cfcNepMfccNv2sQrLp1m0CKxu80jSqHZLoKVL0R0VsZ  
8dMECLLigDlPKRiSyLEr114tErX4/zbkUaWMMR0028kFbTbubQ8YoHlRUwsKW1xLg  
vfi0gRkG/zHXRFQHjX/8NstV7hXlehn7/Gy2EKpSRFhadm/iUHAfmCMkMgHTU248  
JER9+nsX1td59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGHMBPVwbVUD  
A40CiQBvdCoGtPjya1L28xoS3H0ILFCnwQ0r6u0HwleNJPghq78HUyH6Hwxnh0b0  
5o163r6wTFZn5cM0xpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD  
T4JhZ0h/CfcV2WWvhpQugky0pWrZ+EIMneB1dZB96mJVLx0i1480eSgi0PxsZMni  
YM33rTpWQT5Wq0sEyDwUqpne5b8Kkt/s7EN0LJNnPyJJRL1Lcq0dr6j+6YqRtPa7  
a9oWJqMcuTP+bqzGRJh+3HDlFBw2Yzp9iadv4KmB2MzhStLUoi2MSjvnnkdd5Led  
sshAd6WbKff7kLAHQHT4Ai6dMEO4EKKEVf9JBtxCR4JEn6C98Lpg+Lk+rFY7gH0f  
ZxtgURwgXRY3aLurdT55ZKkg3ExVKPzi5EhdpAau7JKhp0wyKozAp/OKWMNrz6h  
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgVvaA8pZCYqxxjpLjSJR8B  
Bu9H9xkTh7K1hxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF  
W6PjBucP0YPp00VtWtQdZZ3df1P0hZ7qvKw0PFA+gKZSckgqASfygiP9V3Zc8jIi  
wjNzoDM2QT+UUJKiGYXJUE009hXzFHlGj759DcNRhpg15AgR57ofISD9yBuCAJY  
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaL0XfzyfyaSmyhsH253tnyL1MejC+2bR  
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82  
HhggcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXypJdyoaX7tDmVc1Lhw19ps/  
0841pIsNLJWXvwxG6B+3LN/kw4Qjwn194Popi0D7+oDm5mht078CrBrRxHMD/0Q  
qniZjKzSZepx1Zq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm  
p8wyik/BlnxN9eKbdT0i2wIi64h2QG8n0k66wQ/PSIJYwZ16eDNEQSzH/1mGCfU  
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVPGXZD0  
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jii3guhdeyRVf100x369kKWcG75q77hxE  
IzSzDyU1BNbnom9SIj3r+qVYmWONatC6q/4D0I42Lnd3dEyZx7jmH3g/S2ASM  
FzWr9pvXc61dsY0kdZ4PYa9XPUZxxFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq  
hkiG9w0BCRUxFgQUwW05DorvVWYF3BWUmAw0rUEajScwfTBtMEkGCSqGSIB3DQEF  
DjA8MCwGCSqGSIB3DQEFDDAfBAhvRzW4sC4xcwICCAECASAwDAYIKoZIhvcNAgkF  
ADAMBggqhkiG9w0CCQUABC6pW2F0dcCNj87zS64NUXG36K5aXdnFHctIk5Bf4kG  
3QqITk9UIFVTRUQCAgga

### A.5. Invalid PKCS #12 File with Incorrect Salt

The following base64-encoded PKCS #12 file **MUST NOT** be readable by an implementation following this RFC when it is verifying integrity protection.

```
MIIKigIBAzCCCgUGCSqGSIB3DQEHAaCCCFYEggnymIIJ7jCCBGIGCSqGSIB3DQEH
BqCCBFMwggRPAgEAMIIIESAYJKoZIHvcNAQcBMFcGCSqGSIB3DQEFDTBKMCKGCSqG
SIb3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIHvcNAGkFADAdBg1ghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPHVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8g0zBMFf6BpXf/3xWAJtxyic+tSNETF0Ja8zTZb0+1V0w9
5eUmDrPUpuxEVbb0KJtIc63gRkcfRtDd6Ii4Zzbzj2Evr4/S4hnrQBsirYVzJWY
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDC0y0ZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLkmZoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQ1hJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46h0f4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0Qc0i29/M9WwF1o4urePyI8PK2qtVAmPd3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQq0jsQCxVz9i9K8NDeD
aau98VA10To2sk3/VR/QUq0PRwU1jPN5BzUevhE7S0y/ImuJKwpGqqFljYdrQmj5
jDe+LmYH9QGVR1fN8zuU+48FY8CAoeBeHn5AAPm10PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWekj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
lDoXvvS3NqsnTXHcn3T9tkPRoe6L7Dh3x40d961cRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF
c7hLNQuuaF4qoDaVwYXHH3iuX6Y1J/3siTKbYCVXPEZ0AMBP91F/OU76UMJBQNFU
0xjDx+3AhUVgnGuCsmY1K6ETDp8q0ZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkcZHi4C2fXnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXqTqwEuvzGHLVfScaAde40ZFBmtBrf70wG7Zk08SUZ8Zz1IX3+S024g7yJ
QRev/6x6TtkwggWEbGkqhkiG9w0BBWgGggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFCGCSqGSIB3DQEFDTBKMCKGCSqGSIB3DQEFDDAcBAHtxzw+
VptrYAICCAAwDAYIKoZIHvcNAGkFADAdBg1ghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdTQEGgTQzCwI7j34gCTvfj6nuOSndAjShGv7mN2j7WMV0ps1Tpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pd0cFcnEpMFccNv2sQrLp1m0CKXu80jSqHZLoKVL0R0VsZ
8dMECLLigDlPKRiSyLEr114tErX4/zbkUaWMMR0028kFbTbubQ8YoHLRUwsKW1xLg
vfi0gRKG/zHXRFQHjX/8NstV7hX1ehn7/Gy2EKPSRFhadm/iUHAfmCMkMgHTU248
JER9+nsX1td59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGHMBPVwbVUD
A40CiQBvDcoGtPjya1L28xoS3H0ILFCnwQ0r6u0HwleNJPGHq78HUyH6Hwxnh0b0
5o163r6wTFZn5cM0xpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
T4JhZ0h/CfcV2WWvhpQugky0pWrZ+EIMneB1dZB96mJVLx0i1480eSgi0PsxZMni
YM33rTpwQT5Wq0sEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1Lcq0dr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HD1FBw2Yzp9iadV4KmB2MzhStLUoi2MSjvnnkkd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKKEVF9JBtxCR4JEn6C98Lpg+Lk+rFY7gH0f
ZxtgGURwgXRY3aLurdT55ZKgk3ExVKPzi5EhdPaau7JKhp0wyKozAp/OKWMNrz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8YgFhGvVaA8pZCYqxxjpLjSJR8B
Bu9H9xkTh7K1hxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF
W6PJbucP0YPp00VtWtQdZZ3df1P0hZ7qKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
wjNzoDM2QT+UUJKiGyXJUE009hxzFHLGj759DcNRhpg15AgR57ofISD9yBuCAJY
PQ/aZHPFuRtrcVG3RaIbCAS73nEznKyFaL0XfzyfyasmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82
HhggcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYpJdyoaX7tDmVc1Lhw19ps/
0841pIsNLJWXwvxG6B+3LN/kw4Qjwn194Popi0D7+oDm5mhtT078CrBrRxHMD/0Q
qniZjKzSzepx1Zq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/B1ndxN9eKbdT0i2wi64h2QG8n0k66wQ/PSIJYwZ16eDNEQSZH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVPgXZD0
```

```
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiiig3guhdeyRVf100x369kKWcG75q77hxE
IzSzDyU1BNbnom9SIj3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsY0kdZ4PYa9XPUZxxFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq
hkiG9w0BCRUxFgQUwW05DorvVWYF3BWUmAw0rUEajScwfdBtMEkGCSqGSIB3DQEF
DjA8MCwGCSqGSIB3DQEFDDAfbAHOt1QgVVFRAICCAACASAwDAYIKoZIhvcNAgkF
ADAMBggqhkiG9w0CCQUABCB6pW2F0dcCNj87zS64NUXG36K5aXDnFHctIk5Bf4kG
3QQIb0c80LAuMXMCAQE=
```

## A.6. Invalid PKCS #12 File with Missing Key Length

The following base64-encoded PKCS #12 file **MUST NOT** be readable by an implementation following this RFC when it is verifying integrity protection.

```
MIIKiAIBAzCCCgUGCSqGSIB3DQEHAAcccFYeggnymIIJ7jCCBGIGCSqGSIB3DQEH
BqCCBFMwggRPAgEAMIIIESAYJKoZIhvcNAQcBMFcgCSqGSIB3DQEFDTBKMCKGCSqG
SIb3DQEFDDAcBAG9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xocF76DtVPhVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8g0zBMFf6BpXf/3xWAJtxyic+tSNETF0Ja8zTZb0+1V0w9
5eUmDrPUpxEVbb0KJtIc63gRkcfrPtDd6Ii4Zzbzj2Evr4/S4hnrQBsiryVzJWY
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDC0yOZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLkMzoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQ1hJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46h0f4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0Qc0i29/M9WwFlo4urePyI8PK2qtVampD3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQq0jsQCxVz9i9K8NdeD
aau98VA10To2sk3/VR/QUq0PRwU1jPN5BzUevhE7S0y/ImuJKwpGqqFljYdrQmj5
jDe+LmYH9QGVr1fn8zuU+48FY8CAoeBeHn5AAPm10PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWekj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
lDoXvvS3NqsnTXHcn3T9tkPRoe6L7Dh3x40d961cRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF
c7hLNquuaF4qoDaVwYXHH3iuX6Y1J/3siTKbYCVXPEZOAMP91F/OU76UMJBQNFU
0xjDx+3AhUVgnGuCsmY1K6ETDp8qOZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkczHi4C2fxnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXdQTWqEuvzGHLVFsCuAde40ZFBmtBrf70wG7Zk08SUZ8Zz1IX3+S024g7yj
QRev/6x6TtkwggWEBGkqhkiG9w0BBwGggv1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFCGCSqGSIB3DQEFDTBKMCKGCSqGSIB3DQEFDDAcBAHtxzw+
VptrYAIICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdtQEggTQzCwI7j34gCTvfj6nu0SndAjShGv7mN2j7WMV0ps1Tpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pd0cfCnEpMFccNv2sQrLp1m0CKXu80jSqHZLoKVL0R0VsZ
8dMECLLigD1PKRiSyLEr114tErX4/zbkUaWMMR0028kFbTbubQ8YoH1RUwsKW1xLg
vfi0gRkG/zHXRFQHjX/8NStv7hX1ehn7/Gy2EKPsRFhadm/iUHAfmCMkMgHTU248
JER9+nsX1td59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGhMBPVwbVUD
A40CiQBvdCoGtPjya1L28xoS3H0ILFCnwQ0r6u0Hw1eNJPghq78HUyH6Hwxnh0b0
5o163r6wTFZn5cM0xpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
T4JhZ0h/CfcV2WWvhPQuqgY0pWrZ+EIMneB1dZB96mJVLx0i1480eSgi0PsxZMni
YM33rTpwQT5Wq0sEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1LcqOdr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HD1FBw2Yzp9iadv4KmB2MzhStLUoi2MSjvnnkkd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKkEVF9JBtxCR4JEn6C98Lpg+Lk+rFY7gH0f
ZxtgURwgXRY3aLUsYrdT55ZKgk3ExVKPzi5EhdpaAu7JKhp0wyKozAp/OKWMNrz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgvVvaA8pZCYqxxjpLjSJrR8B
Bu9H9xkTh7K1hxgreXyV19uAYbUd95kcox9izad6VPnovgFSb+0mdy6PJACPj6hF
W6PJbucP0YPp00VtWtQdZZ3df1P0hZ7qvKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
```

```
wjNzoDM2QT+UUJKiiGYXJUE009hXzFH1Gj759DcNRhpgl5AgR57ofISD9yBuCAJY
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaL0XfzyfyaSmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rrroQpZBX82
HhggcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYPjdyoaX7tDmVc1Lhw19ps/
0841pIsNLJWXwvxG6B+3LN/kw4QjwN194Popi0D7+oDm5mhtt078CrBrRxHMD/0Q
qniZjKzSZepxLZq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/BlndxN9eKbdT0i2wIi64h2QG8n0k66wQ/PSIJYwZl6eDNEQSZH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVPGXZD0
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiig3guhdeyRVf100x369kKWcG75q77hxE
IzSzDyU1BNbnom9SIjut3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsY0kdZ4PYa9XPUZxxFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq
hkiG9w0BCRUxFgQUwW05DorvVWYF3BWUmAw0rUEajScwejBqMEYGCsqGSib3DQEF
DjA5MCKGCSqGSib3DQEFDDAcBAhVrZw4sC4xcwICCAAWDAYIKoZIhvcNAgkFADAM
BggqhkiG9w0CCQUACB6pW2F0dcCNj87zS64NUXG36K5aXDNFHctIk5Bf4kG3QQI
b0c80LAuMXMCAgGA
```

## Appendix B. ASN.1 Module

This appendix documents ASN.1 [\[x680\]](#) [\[x681\]](#) [\[x682\]](#) [\[x683\]](#) [\[x690\]](#) types, values, and object sets for this specification. It does so by providing an ASN.1 module called PKCS12-PBMAC1-2023.

Combine this module with the PKCS-12 ASN.1 module found in [Appendix D](#) of [\[RFC7292\]](#) and the pkcs5v2-1 ASN.1 module in [Appendix C](#) of [\[RFC8018\]](#) to add SHA-2-based HMACs by replacing the PBKDF2-PRFs class referenced from [\[RFC7292\]](#).

```
PKCS12-PBMAC1-2023
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    smime(16) id-mod(0) id-pkcs12-pbmac1-2023(76) }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS

AlgorithmIdentifier, ALGORITHM-IDENTIFIER, rsadsi
  FROM PKCS5v2-1 -- From [RFC8018]
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-5(5)
    modules(16) pkcs5v2-1(2) }
;

-- object identifier arcs

pkcs OBJECT IDENTIFIER ::= { rsadsi 1 }

pkcs-5 OBJECT IDENTIFIER ::= { pkcs 5 }

digestAlgorithm OBJECT IDENTIFIER ::= { rsadsi 2 }

-- HMAC object identifiers

id-hmacWithSHA1 OBJECT IDENTIFIER ::= { digestAlgorithm 7 }

id-hmacWithSHA224 OBJECT IDENTIFIER ::= { digestAlgorithm 8 }
```

```

id-hmacWithSHA256 OBJECT IDENTIFIER ::= { digestAlgorithm 9 }
id-hmacWithSHA384 OBJECT IDENTIFIER ::= { digestAlgorithm 10 }
id-hmacWithSHA512 OBJECT IDENTIFIER ::= { digestAlgorithm 11 }
id-hmacWithSHA512-224 OBJECT IDENTIFIER ::= { digestAlgorithm 12 }
id-hmacWithSHA512-256 OBJECT IDENTIFIER ::= { digestAlgorithm 13 }

-- PBKDF2-PRF algorithm identifiers
PBKDF2-PRFs ALGORITHM-IDENTIFIER ::= {
  { NULL IDENTIFIED BY id-hmacWithSHA1 }           |
  { NULL IDENTIFIED BY id-hmacWithSHA224 }         |
  { NULL IDENTIFIED BY id-hmacWithSHA256 }         |
  { NULL IDENTIFIED BY id-hmacWithSHA384 }         |
  { NULL IDENTIFIED BY id-hmacWithSHA512 }         |
  { NULL IDENTIFIED BY id-hmacWithSHA512-224 }     |
  { NULL IDENTIFIED BY id-hmacWithSHA512-256 },
  ...
}

-- HMAC algorithm identifiers
algid-hmacWithSHA1 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA1, parameters NULL : NULL }

algid-hmacWithSHA224 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA224, parameters NULL : NULL }

algid-hmacWithSHA256 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA256, parameters NULL : NULL }

algid-hmacWithSHA384 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA384, parameters NULL : NULL }

algid-hmacWithSHA512 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA512, parameters NULL : NULL }

algid-hmacWithSHA512-224 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA512-224, parameters NULL : NULL }

algid-hmacWithSHA512-256 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
  { algorithm id-hmacWithSHA512-256, parameters NULL : NULL }

-- PBMAC1-params
PBMAC1-params ::= SEQUENCE {
  keyDerivationFunc AlgorithmIdentifier {{PBMAC1-KDFs}},
  messageAuthScheme AlgorithmIdentifier {{PBMAC1-MACs}} }

PBMAC1-KDFs ALGORITHM-IDENTIFIER ::= {
  { PBKDF2-params IDENTIFIED BY id-PBKDF2},
  ...
}

```

```
PBMAC1-MACs ALGORITHM-IDENTIFIER ::= { ... }
id-PBKDF2 OBJECT IDENTIFIER ::= { pkcs-5 12 }
PBKDF2-params ::= SEQUENCE {
  salt CHOICE {
    specified OCTET STRING,
    otherSource AlgorithmIdentifier {{PBKDF2-SaltSources}}
  },
  iterationCount INTEGER (1..MAX),
  keyLength INTEGER (1..MAX) OPTIONAL,
  prf AlgorithmIdentifier {{PBKDF2-PRFs}} DEFAULT algid-hmacWithSHA1
}
PBKDF2-SaltSources ALGORITHM-IDENTIFIER ::= { ... }
END
```

## Author's Address

**Alicja Kario**

Red Hat, Inc.

Purkynova 115

61200 Brno

Czech Republic

Email: [hkario@redhat.com](mailto:hkario@redhat.com)